Seguridad de vSphere

Actualización 3

VMware vSphere 8.0
VMware ESXi 8.0
vCenter Server 8.0



Puede encontrar la documentación técnica más actualizada en el sitio web de VMware by Broadcom en:

https://docs.vmware.com/es/

VMware by Broadcom
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contenido

Acerca de la seguridad de vSphere

Seguridad de vSphere proporciona información sobre cómo proteger el entorno de vSphere® para VMware® vCenter® Server y VMware ESXi.

En VMware, valoramos la inclusión. Para fomentar este principio dentro de nuestra comunidad de clientes, socios y personal interno, creamos contenido con un lenguaje inclusivo.

A modo de ayuda para proteger el entorno de vSphere, en esta documentación se describen las características de seguridad disponibles y las medidas que se pueden adoptar para proteger el entorno contra ataques.

Tabla 1-1. Información destacada de *Seguridad de vSphere*

Temas	Contenido destacado
Administración de usuarios y permisos	■ Modelo de permisos (funciones, grupos y objetos). ■ Crear funciones personalizadas. ■ Crear permisos. ■ Administrar permisos globales.
Características de seguridad del host	■ Modo de bloqueo y otras funciones del perfil de seguridad ■ Autenticación de la tarjeta inteligente del host ■ vSphere Authentication Proxy ■ Arranque seguro UEFI ■ Módulo de plataforma de confianza (Trusted Platform Module, TPM) ■ VMware® vSphere Trust Authority™. ■ Configuración ESXi segura y sellado de configuración
Cifrado de máquinas virtuales	■ VMware vSphere® Proveedor de claves nativas™. ■ Funcionamiento del cifrado de máquinas virtuales ■ Configuración de KMS ■ Cifrado y descifrado de máquinas virtuales ■ Solución de problemas y prácticas recomendadas
Seguridad del sistema operativo invitado	■ Módulo de plataforma de confianza virtual (Virtual Trusted Platform Module, vTPM) ■ Seguridad basada en virtualización (Virtualization Based Security, VBS)
Administrar la configuración del protocolo TLS	Cambio de la configuración del protocolo TLS mediante una utilidad de línea de comandos.

Tabla 1-1. Información destacada de *Seguridad de vSphere* (continuación)

Temas	Contenido destacado
Prácticas recomendadas y fortalecimiento de la seguridad	Prácticas recomendadas y consejos de expertos en seguridad de VMware. ■ Seguridad de vCenter Server ■ Seguridad de los hosts ■ Seguridad de las máquinas virtuales ■ Seguridad de las redes
Privilegios de vSphere	Lista completa de todos los privilegios de vSphere admitidos en esta versión.

Documentación relacionada

En un documento complementario, *vSphere Authentication*, se explica cómo se pueden utilizar los servicios de autenticación para, por ejemplo, administrar la autenticación con vCenter Single Sign-On y administrar certificados en el entorno de vSphere.

Además de estos documentos, VMware publica la *guía de configuración de seguridad de vSphere* (anteriormente denominada la *Guía de fortalecimiento*) para cada versión de vSphere. Puede obtener dicha guía en https://core.vmware.com/security. La *guía de configuración de seguridad de vSphere* contiene directrices de configuración de seguridad que el cliente puede o debe definir, así como la configuración de seguridad proporcionada por VMware que el cliente debe auditar para garantizar que aún tiene el valor predeterminado.

Qué ocurrido con Platform Services Controller

A partir de vSphere 7.0, la implementación de una nueva instancia de vCenter Server o la actualización a vCenter Server 7.0 requiere el uso de vCenter Server Appliance, una máquina virtual preconfigurada y optimizada para ejecutar vCenter Server. La nueva instancia de vCenter Server contiene todos los servicios de Platform Services Controller y conserva la funcionalidad y los flujos de trabajo, incluidos la autenticación, la administración de certificados, las etiquetas y la concesión de licencias. Ya no es necesario ni es posible implementar y utilizar una instancia de Platform Services Controller externa. Todos los servicios de Platform Services Controller se consolidan en vCenter Server, y se simplifican la implementación y la administración.

Dado que estos servicios ahora forman parte de vCenter Server, ya no se describen como parte de Platform Services Controller. En vSphere 7.0, la publicación de *vSphere Authentication* reemplaza la publicación de *Administrar Platform Services Controller*. La nueva publicación contiene información completa sobre la autenticación y la administración de certificados. Para obtener información sobre la actualización o la migración de las implementaciones de vSphere 6.5 y 6.7 con una instancia externa existente de Platform Services Controller a vSphere 7.0 mediante vCenter Server Appliance, consulte la documentación de *Actualizar vSphere*.

Audiencia prevista

Esta información está destinada a administradores de sistemas con experiencia que estén familiarizados con la tecnología de máquinas virtuales y las operaciones de centros de datos.

Certificaciones

VMware difunde una lista pública de productos de VMware que hayan completado certificaciones de criterios comunes. Para comprobar si se certificó una versión de un producto de VMware en particular, consulte la página web de evaluación y validación de criterios comunes: https://www.vmware.com/security/certifications/common-criteria.html.

Seguridad en el entorno de vSphere

1

Los componentes de un entorno de vSphere vienen protegidos desde el inicio mediante varias características, como la autenticación, la autorización, un firewall en cada host ESXi, etc. La configuración predeterminada se puede modificar de muchas formas. Por ejemplo, puede establecer permisos en objetos de vCenter Server, abrir puertos de firewall o cambiar los certificados predeterminados. Es posible tomar medidas de seguridad para diferentes objetos de vSphere, por ejemplo, sistemas vCenter Server, hosts ESXi, máquinas virtuales, y objetos de redes y de almacenamiento.

La descripción general detallada de las diferentes áreas de vSphere que requieren atención permite planificar la estrategia de seguridad. También se pueden aprovechar otros recursos de seguridad de vSphere disponibles en el sitio web de VMware.

Lea los siguientes temas a continuación:

Proteger hipervisor de ESXi

El hipervisor de ESXi ya viene protegido. Puede aumentar la protección de los hosts ESXi con el modo de bloqueo y otras características integradas. A los fines de coherencia, puede configurar un host de referencia y mantener todos los hosts sincronizados con el perfil de host del host de referencia. También puede proteger el entorno con la administración generada por script para garantizar que los cambios se apliquen a todos los hosts.

Puede mejorar la protección de los hosts ESXi administrados por vCenter Server mediante las siguientes acciones. Los parámetros de seguridad de los hosts individuales son similares, pero las tareas de administración pueden ser diferentes. Consulte la documentación de *Administrar un host único de vSphere: VMware Host Client*.

Limitar el acceso a ESXi

De forma predeterminada, los servicios de ESXi Shell y SSH no se ejecutan, y solo el usuario raíz puede iniciar sesión en la interfaz de usuario de la consola directa (DCUI). Si decide habilitar el acceso a ESXi o SSH, puede establecer los tiempos de espera para reducir el riesgo de que se produzca un acceso no autorizado. Los usuarios que pueden acceder al host ESXi deben tener permisos para administrar el host. Puede establecer permisos en el objeto de host del sistema vCenter Server que administra el host.

Consulte Usar ESXi Shell.

Utilización de usuarios designados y privilegio mínimo

De manera predeterminada, el usuario raíz puede realizar muchas tareas. No permita que los administradores inicien sesión en el host ESXi con la cuenta de usuario raíz. En su lugar, cree usuarios administradores designados de vCenter Server y asigne la función de administrador a dichos usuarios. También puede asignar una función personalizada a esos usuarios. Consulte Crear una función personalizada de vCenter Server.

Si administra usuarios directamente en el host, las opciones de administración de funciones son limitadas. Consulte la documentación de *Administrar un host único de vSphere: VMware Host Client*.

Reducción de la cantidad de puertos de firewall de ESXi abiertos

De forma predeterminada, los puertos de firewall del host ESXi se abren solo cuando se inicia el servicio correspondiente. Se pueden utilizar los comandos de vSphere Client, ESXCLI o PowerCLI para comprobar y administrar el estado de los puertos de firewall.

Consulte Configurar el firewall de ESXi.

Automatización de la administración de hosts ESXi

Ya que generalmente es importante que diferentes hosts del mismo centro de datos estén sincronizados, utilice la instalación generada por script o vSphere Auto Deploy para aprovisionar los hosts. Los hosts se pueden administrar con los scripts. Los perfiles de host son una alternativa a la administración generada por script. Se debe configurar un host de referencia, exportar el perfil de host y aplicar el perfil de host a todos los hosts. El perfil de host se puede aplicar directamente o como parte del aprovisionamiento con Auto Deploy.

Consulte Usar scripts para administrar opciones de configuración de hosts ESXi y la documentación *Instalar y configurar vCenter Server* para obtener información sobre vSphere Auto Deploy.

Aprovechar el modo de bloqueo de ESXi

En el modo de bloqueo, solo se puede acceder a los hosts ESXi a través de vCenter Server de forma predeterminada. Puede seleccionar el modo de bloqueo estricto o el modo de bloqueo normal. Puede definir usuarios con excepción para permitir el acceso directo a las cuentas de servicio, como los agentes de copia de seguridad.

Consulte Configurar y administrar el modo de bloqueo en hosts ESXi.

Comprobación de la integridad de los paquetes de VIB

Cada paquete del paquete de instalación de vSphere (vSphere Installation Bundle, VIB) tiene un nivel de aceptación asociado. Es posible agregar un VIB a un host ESXi solo si el nivel de aceptación de VIB es el mismo o mejor que el nivel de aceptación del host. No se puede agregar un VIB CommunitySupported o PartnerSupported a un host a menos que se cambie de forma explícita el nivel de aceptación del host.

Consulte Administrar los niveles de aceptación de los hosts ESXi y los paquetes de instalación de vSphere.

Administrar certificados de ESXi

VMware Certificate Authority (VMCA) aprovisiona cada host ESXi con un certificado firmado cuya entidad de certificación raíz predeterminada es VMCA. Si las directivas de la empresa lo requieren, puede reemplazar los certificados existentes con certificados firmados por una entidad de certificación empresarial o externa.

Consulte Administrar certificados para hosts ESXi.

Considerar la autenticación de tarjeta inteligente para ESXi

ESXi admite el uso de la autenticación de tarjeta inteligente en lugar de la autenticación mediante nombre de usuario y contraseña. También se admite la autenticación en dos fases para vCenter Server. Puede configurar al mismo tiempo la autenticación con nombre de usuario y contraseña, y la autenticación de tarjeta inteligente.

Consulte Configurar y administrar la autenticación de tarjeta inteligente para ESXi.

Considerar el bloqueo de cuentas de ESXi

Se admite el bloqueo de cuentas para el acceso a través de SSH y vSphere Web Services SDK. De forma predeterminada, se permite un máximo de cinco intentos con errores antes de que la cuenta se bloquee. De forma predeterminada, la cuenta se desbloquea después de 15 minutos.

Nota La interfaz de la consola directa (DCUI) y ESXi Shell no admiten el bloqueo de cuentas.

Consulte Bloqueo de cuenta y contraseñas ESXi.

Proteger los sistemas vCenter Server y los servicios asociados

La autenticación mediante vCenter Single Sign-On y la autorización mediante el modelo de permisos de vCenter Server protegen el sistema vCenter Server y los servicios asociados. Es posible modificar el comportamiento predeterminado y tomar medidas para limitar el acceso al entorno.

Cuando proteja el entorno de vSphere, tenga en cuenta que se deben proteger todos los servicios que están asociados con las instancias de vCenter Server. En algunos entornos, es posible que se protejan varias instancias de vCenter Server.

vCenter Server utiliza comunicación cifrada

De forma predeterminada ("listo para usar"), se cifra toda la comunicación de datos entre el sistema vCenter Server y los demás componentes de vSphere. En algunos casos, según cómo configure su entorno, es posible parte del tráfico no esté cifrado. Por ejemplo, puede configurar SMTP sin cifrar para las alertas de correo electrónico y SNMP sin cifrar para la supervisión. El tráfico de DNS también está sin cifrar. vCenter Server escucha en los puertos 80 (TCP) y 443 (TCP). El puerto 443 (TCP) es el puerto HTTPS estándar del sector (HTTP seguro) y utiliza el cifrado TLS para protegerse. Consulte Capítulo 15 Configuración de vSphere TLS. El puerto 80 (TCP) es el puerto HTTP estándar del sector y no utiliza cifrado. El propósito del puerto 80 es redireccionar las solicitudes del puerto 80 al puerto 443, donde son seguras.

Proteger sistemas vCenter Server

El primer paso para proteger el entorno de vCenter Server es fortalecer cada equipo en el que se ejecutan vCenter Server o un servicio asociado. El enfoque es similar cuando se trata de una máquina física o una máquina virtual. Siempre instale las revisiones de seguridad más recientes para el sistema operativo y siga las prácticas recomendadas estándar de la industria para proteger el equipo host.

Información sobre el modelo de certificado de vSphere

De forma predeterminada, VMware Certificate Authority (VMCA) aprovisiona a cada host ESXi y cada máquina del entorno con un certificado firmado por VMCA. Si la directiva de su empresa lo requiere, puede cambiar el comportamiento predeterminado. Consulte la documentación de *vSphere Authentication* para obtener detalles.

Para mejorar la protección, quite explícitamente los certificados caducados o revocados y las instalaciones con errores.

Configuración de vCenter Single Sign-On

vCenter Server y los servicios asociados están protegidos con el marco de autenticación de vCenter Single Sign-On. Cuando instale el software por primera vez, especifique una contraseña para el administrador del dominio de vCenter Single Sign-On, administrator@vsphere.local de manera predeterminada. Solo ese dominio está inicialmente disponible como un origen de identidad. Puede agregar un proveedor de identidad externo, como los servicios de federación de Active Directory (AD FS) de Microsoft, para la autenticación federada. Es posible agregar otros orígenes de identidad, ya sea de Active Directory o LDAP, y establecer un origen de identidad predeterminado. Los usuarios que se pueden autenticar en uno de esos orígenes de identidad pueden ver objetos y realizar tareas si tienen la autorización para hacerlo. Consulte la documentación de *vSphere Authentication* para obtener detalles.

Nota Se recomienda utilizar la autenticación federada a medida que vSphere avanza hacia la autenticación basada en token. vCenter Server sigue teniendo cuentas locales para acceso administrativo y recuperación de errores.

Asignar funciones de vCenter Server a usuarios o grupos designados

Para mejorar el registro, asocie los permisos que otorga a un objeto con un usuario o grupo designado, y una función predefinida o personalizada. El modelo de permisos de vSphere es muy flexible porque ofrece varios modos de autorizar usuarios o grupos. Consulte Descripción de la autorización en vSphere y Privilegios de vCenter Server necesarios para la realización de tareas comunes.

Restrinja los privilegios de administrador y el uso de la función de administrador. De ser posible, no utilice el usuario administrador anónimo.

Configurar el protocolo de hora de precisión o el protocolo de tiempo de red

Configure el protocolo de hora de precisión (Precision Time Protocol, PTP) o el protocolo de tiempo de red (Network Time Protocol, NTP) para cada nodo del entorno. La infraestructura de certificados de vSphere requiere una marca de tiempo precisa y no funciona correctamente si los nodos no están sincronizados.

Consulte Sincronizar los relojes en la red de vSphere.

Proteger máquinas virtuales

Para proteger las máquinas virtuales, mantenga revisados los sistemas operativos invitados y proteja el entorno virtual como si fuera una máquina física. Considere la posibilidad de desactivar las funcionalidades innecesarias, minimizar el uso de la consola de la máquina virtual y seguir las prácticas recomendadas.

Proteger el sistema operativo invitado

Para proteger el sistema operativo invitado, asegúrese de utilizar las revisiones más recientes y, si corresponde, las aplicaciones antispyware y antimalware. Consulte la documentación del proveedor del sistema operativo invitado. También puede consultar otra información disponible en libros o en Internet para el sistema operativo.

Desactivar la funcionalidad de máquina virtual innecesaria

Compruebe que las funcionalidades innecesarias estén desactivadas para minimizar los puntos de ataque potenciales. Muchas de las características que no se usan con frecuencia se desactivan de manera predeterminada. Quite el hardware que no necesite y desactive ciertas funciones, como Host-Guest Filesystem (HGFS), o bien copie y pegue entre la máquina virtual y una consola remota.

Consulte Desactivar funciones innecesarias en máquinas virtuales.

Usar plantillas de máquinas virtuales y administración generada por scripts

Las plantillas de máquinas virtuales permiten configurar el sistema operativo de manera que se adapte a los requisitos y crear otras máquinas virtuales con la misma configuración.

Si quiere cambiar la configuración de la máquina virtual después de la implementación inicial, considere la opción de usar scripts de PowerCLI. En la mayoría de los casos, en esta documentación se explica cómo realizar tareas mediante vSphere Client. Considere la opción de usar scripts en lugar de vSphere Client para mantener la coherencia de su entorno. En los entornos de gran tamaño, puede agrupar las máquinas virtuales en carpetas para optimizar el proceso de scripting.

Para obtener información sobre las plantillas, consulte Usar plantillas para implementar máquinas virtuales y la documentación de *Administrar máquinas virtuales de vSphere*. Para obtener información sobre PowerCLI, consulte la documentación de VMware PowerCLI.

Minimizar el uso de la consola de la máquina virtual

La consola de máquina virtual cumple la misma función en la máquina virtual que el monitor de un servidor físico. Los usuarios que tienen acceso a una consola de máquina virtual pueden acceder a la gestión de energía de la máquina virtual y a controles de conectividad del dispositivo extraíble. Como resultado, el acceso a la consola de máquina virtual puede permitir un ataque malicioso en la máquina virtual.

Considerar el arranque seguro UEFI para máquinas virtuales

Puede configurar las máquinas virtuales para que utilicen el arranque UEFI. Si el sistema operativo admite el arranque seguro UEFI, puede seleccionar la opción para las máquinas virtuales a fin de aumentar la seguridad. Consulte Activar o desactivar el arranque seguro UEFI para una máquina virtual.

Proteger la capa de redes virtuales

La capa de redes virtuales incluye adaptadores de red virtual, conmutadores virtuales, conmutadores virtuales distribuidos, y puertos y grupos de puertos. ESXi se basa en la capa de redes virtuales para establecer las comunicaciones entre las máquinas virtuales y sus usuarios. Asimismo, ESXi utiliza la capa de redes virtuales para comunicarse con SAN iSCSI, el almacenamiento NAS, etc.

vSphere incluye la matriz completa de características necesarias para una infraestructura segura de redes. Puede proteger cada elemento de la infraestructura por separado, como los conmutadores virtuales, los conmutadores virtuales distribuidos y los adaptadores de red virtuales. Por otra parte, considere las siguientes instrucciones, que se analizan más detalladamente en Capítulo 13 Proteger las redes de vSphere.

Aislamiento del tráfico de red

El aislamiento del tráfico de red es fundamental para proteger el entorno de ESXi. Las distintas redes requieren distintos niveles de aislamiento y acceso. La red de administración aísla los distintos tráficos (tráfico de clientes, de la interfaz de la línea de comandos [Command-Line Interface, CLI] o de la API y del software de terceros) del tráfico normal. Asegúrese de que solo los administradores de sistemas, redes y seguridad puedan acceder a la red de administración.

Consulte Recomendaciones de seguridad para redes de ESXi.

Utilización de firewalls para proteger los elementos de la red virtual

Puede abrir y cerrar los puertos de firewall y proteger cada elemento de la red virtual por separado. Para los hosts ESXi, las reglas de firewall asocian los servicios con los firewalls correspondientes, y pueden abrir y cerrar el firewall de acuerdo con el estado del servicio.

También es posible abrir puertos en instancias de vCenter Server de forma explícita.

Para obtener la lista de todos los puertos y protocolos compatibles en los productos de VMware, incluidos vSphere y vSAN, consulte la herramienta VMware Ports and Protocols™ en https://ports.vmware.com/. Puede buscar puertos por producto de VMware, crear una lista de puertos personalizada e imprimir o guardar listas de puertos.

Consideración de las directivas de seguridad de red

Las directivas de seguridad de redes ayudan a proteger el tráfico contra la suplantación de direcciones MAC y la exploración de puertos no deseada. La directiva de seguridad de un conmutador estándar o distribuido se implementa en la Capa 2 (capa de vínculo de datos) de la pila del protocolo de red. Los tres elementos de la directiva de seguridad son el modo promiscuo, los cambios de dirección MAC y las transmisiones falsificadas.

Consulte la documentación de *Redes de vSphere* para ver las instrucciones.

Protección de las redes de las máquinas virtuales

Los métodos que se utilizan para proteger las redes de máquinas virtuales dependen de varios factores, entre otros:

- El sistema operativo invitado que se está instalado.
- Si las máquinas virtuales funcionan en un entorno de confianza

Los conmutadores virtuales y los conmutadores virtuales distribuidos proporcionan una protección significativa cuando se utilizan junto con otras prácticas de seguridad comunes, como la instalación de firewalls.

Consulte Capítulo 13 Proteger las redes de vSphere.

Consideración de VLAN para proteger el entorno

ESXi es compatible con VLAN de IEEE 802.1q. Las redes VLAN permiten segmentar una red física. Puede utilizar las VLAN para proteger aún más la configuración de la red o el almacenamiento de las máquinas virtuales. Cuando se utilizan redes VLAN, dos máquinas de la misma red física no pueden enviar ni recibir paquetes entre ellas a menos que se encuentren en la misma VLAN.

Consulte Proteger las máquinas virtuales con VLAN.

Protección de las conexiones con el almacenamiento virtualizado

Una máquina virtual almacena archivos del sistema operativo, archivos de aplicación y otros datos en un disco virtual. Cada disco virtual figura en la máquina virtual como una unidad SCSI que está conectada a una controladora SCSI. La máquina virtual está aislada de los detalles de almacenamiento y no puede acceder a la información del LUN donde reside el disco virtual.

Virtual Machine File System (VMFS) es un sistema de archivos distribuidos y un administrador de volúmenes que presenta volúmenes virtuales en el host ESXi. Usted es responsable de proteger la conexión con el almacenamiento. Por ejemplo, si utiliza el almacenamiento iSCSI, puede configurar el entorno para usar el protocolo de autenticación por desafío mutuo (Challenge Handshake Authentication Protocol, CHAP). Si la directiva de la empresa lo requiere, puede configurar CHAP mutuo. Utilice vSphere Client o la CLI para configurar CHAP.

Consulte Prácticas recomendadas de seguridad de almacenamiento.

Evaluar el uso de la seguridad del protocolo de Internet

ESXi admite el protocolo de seguridad de Internet (IPSec) en IPv6. No se puede utilizar IPsec para IPv4.

Consulte Usar el protocolo Internet Protocol Security en hosts ESXi.

Proteger las contraseñas en el entorno de vSphere

La restricción y la caducidad de las contraseñas y el bloqueo de cuentas en el entorno de vSphere dependen de qué sistema el usuario utiliza como destino, quién es el usuario y cómo se establecen las directivas.

Las restricciones de contraseña de ESXi se determinan según ciertos requisitos. Consulte Bloqueo de cuenta y contraseñas ESXi.

vCenter Single Sign-On administra la autenticación de todos los usuarios que inician sesión en vCenter Server y en otros servicios de vCenter. La restricción y la caducidad de las contraseñas y el bloqueo de cuentas dependen de cuál es el dominio del usuario y quién es el usuario.

Contraseña del administrador de vCenter Single Sign-On

La contraseña del usuario administrator@vsphere.local (o del usuario administrator@*midominio* si seleccionó un dominio distinto durante la instalación) no caduca y no está sujeta a la directiva de bloqueo. En los demás casos, la contraseña debe cumplir con las restricciones establecidas en la directiva de contraseñas de vCenter Single Sign-On. Consulte la documentación de *vSphere Authentication* para obtener detalles.

Si olvida la contraseña de este usuario, busque información en la base de conocimientos de VMware sobre la forma de restablecer esta contraseña. El restablecimiento requiere privilegios adicionales, como el acceso raíz al sistema vCenter Server.

Contraseñas para otros usuarios del dominio vCenter Single Sign-On

Las contraseñas de otros usuarios de vsphere.local o de los usuarios del dominio que se especificó durante la instalación deben cumplir con las restricciones establecidas en la directivas de bloqueo y de contraseñas de vCenter Single Sign-On. Consulte la documentación de *vSphere Authentication* para obtener detalles. Estas contraseñas caducan de manera predeterminada a los 90 días. Los administradores pueden cambiar la fecha de caducidad como parte de la directiva de contraseñas.

Si olvida la contraseña de vsphere.local, un usuario administrador puede restablecerla mediante el comando `dir-cli`.

Contraseñas para usuarios de otros orígenes de identidad

La restricción y la caducidad de las contraseñas y el bloqueo de cuentas de todos los demás usuarios se determinan según el dominio (el origen de identidad) en el cual el usuario puede autenticarse.

vCenter Single Sign-On admite un origen de identidad predeterminado. Los usuarios pueden iniciar sesión en el dominio correspondiente con vSphere Client y sus nombres de usuario. Si los usuarios desean iniciar sesión en un dominio no predeterminado, pueden incluir el nombre del dominio, es decir, especificar *user@domain* o *domain\user*. Los parámetros para la contraseña del dominio se aplican a todos los dominios.

Contraseñas de los usuarios de la interfaz de usuario de la consola directa de vCenter Server

vCenter Server Appliance es una máquina virtual preconfigurada que está optimizada para ejecutar vCenter Server y los servicios asociados.

Estas contraseñas se especifican durante la implementación de vCenter Server.

- Contraseña para el usuario raíz.
- Contraseña predeterminada para el administrador del dominio de vCenter Single Sign-On, administrator@vsphere.local.

Es posible cambiar la contraseña del usuario raíz y realizar otras tareas de administración de usuarios locales de vCenter Server desde la interfaz de administración de vCenter Server. Consulte la documentación de *Configuración de vCenter Server*.

Recursos y prácticas recomendadas de seguridad de vCenter Server y ESXi

Si sigue las prácticas recomendadas, los hosts ESXi y los sistemas vCenter Server pueden alcanzar el mismo nivel de seguridad, o incluso uno mayor, que un entorno donde no existe la virtualización.

En este manual se incluyen las prácticas recomendadas para los distintos componentes de la infraestructura de vSphere. Este manual es tan solo una de las fuentes que debe emplear para garantizar un entorno seguro.

Recursos de seguridad de vSphere

"Para obtener más información sobre aspectos específicos de la seguridad de vSphere, utilice el siguiente contenido en este manual".

Tabla 1-1. Prácticas recomendadas de seguridad

Componente de vSphere	Recurso
Host ESXi	Capítulo 3 Proteger hosts ESXi
Sistema vCenter Server	Capítulo 4 Proteger sistemas vCenter Server
Máquina virtual	Prácticas recomendadas de seguridad para las máquinas virtuales
Redes de vSphere	Prácticas recomendadas de seguridad de redes de vSphere

Recursos de seguridad de VMware en la Web

Los recursos de seguridad de VMware, incluidas alertas y descargas, se encuentran disponibles en la Web.

Tabla 1-2. Recursos de seguridad de VMware en la Web

Tema	Recurso
Información sobre seguridad y operaciones de ESXi y vCenter Server, incluidas la configuración segura y la seguridad del hipervisor	https://core.vmware.com/security
Directiva de seguridad de VMware, alertas de seguridad actualizadas, descargas de seguridad y foros de debate sobre temas de seguridad	http://www.vmware.com/go/security
Directiva de respuestas sobre seguridad corporativa	http://www.vmware.com/support/policies/security_response.html VMware se compromete a ayudar en el mantenimiento de un entorno seguro. Los problemas de seguridad se solucionan oportunamente. La directiva de respuestas sobre seguridad de VMware define nuestro compromiso con la solución de posibles vulnerabilidades en nuestros productos.
Directiva de compatibilidad con software externo	http://www.vmware.com/support/policies/ VMware admite diversos sistemas de almacenamiento y agentes de software, como agentes de copia de seguridad, agentes de administración de sistemas, etc. Para consultar las listas de agentes, herramientas y demás opciones de software compatibles con ESXi, busque las guías de compatibilidad de ESXi en http://www.vmware.com/vmtn/resources/. La industria ofrece más productos y opciones de configuración de los que VMware puede probar. Si VMware no incluye un producto o una configuración en una guía de compatibilidad, el soporte técnico intenta ayudarle a resolver los problemas, pero no puede garantizar que se pueda usar el producto o la configuración. Siempre evalúe minuciosamente los riesgos para la seguridad que generan los productos o las opciones de configuración no compatibles.
Normas de seguridad y cumplimiento, así como soluciones de partners y contenido detallado sobre virtualización y cumplimiento	https://core.vmware.com/compliance
Información sobre validaciones y certificados de seguridad como CCEVS y FIPS para diferentes versiones de los componentes de vSphere	https://www.vmware.com/support/support-resources/certifications.html
Guías de configuración de seguridad (anteriormente denominadas guías de fortalecimiento) para diferentes versiones de vSphere y otros productos de VMware	https://core.vmware.com/security-configuration-guide
Informe técnico *Seguridad de VMware vSphere Hypervisor*	http://www.vmware.com/files/pdf/techpaper/vmw-wp-secrty-vsphr-hyprvsr-uslet-101.pdf

Tareas de administración de permisos y usuarios de vSphere

2

La autenticación y la autorización rigen el acceso al entorno de vSphere. vCenter Single Sign-On admite la autenticación, lo cual implica que determina si un usuario puede iniciar sesión o no en los componentes de vSphere. Cada usuario también debe estar autorizado para ver o manipular los objetos de vSphere.

Para obtener una descripción general de la asignación de funciones y permisos mediante vSphere Client, vea el siguiente vídeo.



(Asignar funciones y permisos con vSphere Client)

vCenter Server permite un control detallado de la autorización con permisos y funciones. Cuando se asigna un permiso a un objeto en la jerarquía de objetos de vCenter Server, se especifica qué usuario o grupo tiene cuál privilegio sobre ese objeto. Para especificar los privilegios se usan funciones, que son conjuntos de privilegios.

En un principio, solo el usuario administrador del dominio de vCenter Single Sign-On está autorizado a iniciar sesión en el sistema vCenter Server. El dominio predeterminado es vsphere.local y el administrador predeterminado es administrator@vsphere.local. Puede cambiar el dominio predeterminado durante la instalación de vSphere.

Como usuario administrador, puede:

1 Agregue un origen de identidad en el cual los usuarios y grupos estén definidos en vCenter Single Sign-On. Consulte la documentación de *vSphere Authentication*.

2 Otorgue privilegios a un usuario o un grupo al seleccionar un objeto, como una máquina virtual o un sistema de vCenter Server y asignar una función sobre ese objeto al usuario o al grupo.

Lea los siguientes temas a continuación:

- Usar registrador de privilegios
- Prácticas recomendadas para funciones y permisos de vCenter Server
- Privilegios de vCenter Server necesarios para la realización de tareas comunes

Descripción de la autorización en vSphere

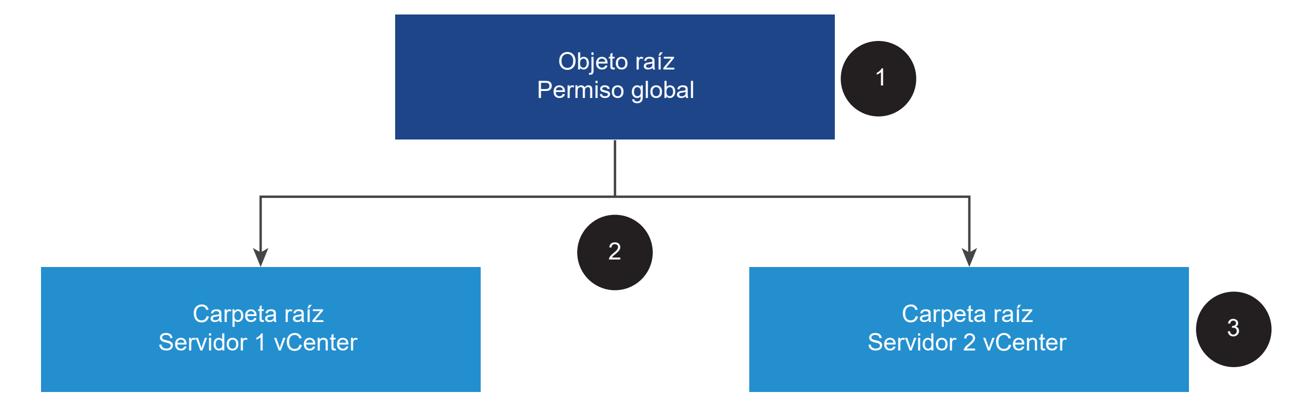
vSphere admite varios modelos para determinar si un usuario puede realizar una tarea. La pertenencia a un grupo en vCenter Single Sign-On determina qué se le permite hacer. Su función respecto de un objeto o su permiso global determinan si se le permite realizar otras tareas.

Cómo funcionan los permisos en vSphere

vSphere permite a los usuarios con privilegios otorgar permisos a otros usuarios para realizar tareas. Se pueden utilizar permisos globales o permisos locales de vCenter Server para autorizar a otros usuarios en las instancias individuales de vCenter Server.

En la siguiente figura, se muestra cómo funcionan los permisos globales y locales.

Figura 2-1. Permisos globales y permisos locales



En esta figura:

1 Asigne un permiso global en el nivel de objeto raíz con la opción "Propagar a objetos secundarios" seleccionada.

2 vCenter Server propaga los permisos a las jerarquías de objetos vCenter Server 1 y vCenter Server 2 en el entorno.

3 Un permiso local en la carpeta raíz de vCenter Server 2 anula el permiso global.

Permisos de vCenter Server

El modelo de permisos de los sistemas vCenter Server se basa en la asignación de permisos a los objetos de la jerarquía de objetos. Los usuarios obtienen permisos de las siguientes maneras.

- Desde un permiso específico para el usuario o desde los grupos de los que el usuario es miembro

- Desde un permiso en el objeto o a través de la herencia de permisos de un objeto principal

Cada permiso otorga un conjunto de privilegios a un usuario o grupo; es decir, asigna una función para un objeto seleccionado. Puede usar vSphere Client para agregar permisos. Por ejemplo, puede hacer clic con el botón secundario en una máquina virtual, seleccionar **Agregar permiso** y completar el cuadro de diálogo para asignar una función a un grupo de usuarios. Esa función proporciona a esos usuarios los privilegios correspondientes sobre la máquina virtual.

Figura 2-2. Agregar permisos a una máquina virtual mediante vSphere Client

Permisos globales

Los permisos globales conceden a un usuario o grupo privilegios para ver o administrar todos los objetos en cada una de las jerarquías de inventario de las soluciones de la implementación. Es decir, los permisos globales se aplican a un objeto raíz global que abarca las jerarquías del inventario de soluciones. (Las soluciones incluyen vCenter Server, VMware Aria Automation Orchestrator, etc.). Los permisos globales también se aplican a objetos globales, como etiquetas y bibliotecas de contenido. Por ejemplo, considere una implementación que consta de dos soluciones: vCenter Server y VMware Aria Automation Orchestrator. Puede utilizar permisos globales para asignar una función a un grupo de usuarios que tenga privilegios de solo lectura para todos los objetos de las jerarquías de objetos de vCenter Server y VMware Aria Automation Orchestrator.

Los permisos globales se replican en el dominio de vCenter Single Sign-On (vsphere.local de forma predeterminada). Los permisos globales no proporcionan autorización para servicios administrados a través de grupos de dominios de vCenter Single Sign-On. Consulte Usar permisos globales de vCenter Server.

Pertenencia a grupos de vCenter Single Sign-On

Los miembros de un grupo de dominios de vCenter Single Sign-On pueden realizar determinadas tareas. Por ejemplo, se puede llevar a cabo la administración de licencias si se es miembro del grupo LicenseService.Administrators. Consulte la documentación de *vSphere Authentication*.

Permisos de hosts locales de ESXi

Si administra un host ESXi independiente que no está administrado por un sistema vCenter Server, puede asignar uno de las funciones predefinidas a los usuarios. Consulte la documentación de *Administrar un host único de vSphere: VMware Host Client*.

Para hosts administrados, asigne funciones al objeto de host ESXi en el inventario de vCenter Server.

Descripción del modelo de permisos de nivel de objetos

Autoriza a un usuario o grupo a realizar tareas en objetos de vCenter Server mediante permisos en el objeto. Desde un punto de vista programático, cuando un usuario intenta realizar una operación, se ejecuta un método de API. vCenter Server comprueba los permisos de ese método para ver si el usuario está autorizado a realizar la operación. Por ejemplo, cuando un usuario intenta agregar un host, se invoca al método `AddStandaloneHost_Task`. Este método requiere que la función del usuario tenga el privilegio Host.Inventory.AddStandaloneHost. Si la comprobación no encuentra este privilegio, se le niega al usuario el permiso para agregar el host.

Los siguientes conceptos son importantes.

Permisos

Cada objeto en la jerarquía de objetos de vCenter Server tiene permisos asociados. Cada permiso especifica en un solo grupo o usuario qué privilegios tiene ese grupo o usuario sobre el objeto. Los permisos se pueden propagar a los objetos secundarios.

Usuarios y grupos

En los sistemas vCenter Server se pueden asignar privilegios solo a usuarios autenticados o a grupos de usuarios autenticados. Los usuarios se autentican mediante vCenter Single Sign-On. Los usuarios y los grupos deben definirse en el origen de identidad que vCenter Single Sign-On utiliza para autenticar. Defina usuarios y grupos utilizando las herramientas en su origen de identidad, por ejemplo, Active Directory.

Privilegios

Los privilegios son controles de acceso detallados. Esos privilegios se pueden agrupar en funciones que se pueden asignar a usuarios o grupos posteriormente.

Funciones

Las funciones son conjuntos de privilegios. Las funciones permiten asignar permisos en un objeto en función de un conjunto típico de tareas que realizan los usuarios. En vCenter Server, las funciones del sistema —tales como Administrador— están predefinidas y no se pueden cambiar. vCenter Server también proporciona algunas funciones de muestra

predeterminadas, como Administrador de grupo de recursos, que se pueden modificar. Se pueden crear funciones personalizadas, ya sea desde cero o mediante la clonación y la modificación de las funciones de muestra. Consulte Crear una función personalizada de vCenter Server.

En la siguiente figura, se muestra cómo se crea un permiso a partir de privilegios y funciones, y se lo asigna a un usuario o grupo para un objeto de vSphere.

Figura 2-3. Permisos de vSphere

Para asignar permisos sobre un objeto, siga estos pasos:

1 Seleccione el objeto en el que desea aplicar el permiso en la jerarquía de objetos de vCenter Server.

2 Seleccione el grupo o el usuario que tendrá los privilegios sobre el objeto.

3 Seleccione privilegios individuales o una función, es decir, un conjunto de privilegios que el grupo o el usuario tendrán sobre el objeto.

   De forma predeterminada, la opción Propagar a objetos secundarios no está seleccionada. Debe activar la casilla para que el grupo o el usuario tengan la función seleccionada para el objeto deseado y sus objetos secundarios.

vCenter Server ofrece funciones de ejemplo, que combinan conjuntos de privilegios de uso frecuente. También puede crear funciones personalizadas mediante la combinación de un conjunto de funciones.

En muchos casos, los permisos deben definirse tanto en un objeto de origen como en un objeto de destino. Por ejemplo, al mover una máquina virtual, se necesitan privilegios en esa máquina virtual, pero también privilegios en el centro de datos de destino.

Consulte la siguiente información.

Para averiguar sobre...	Consulte...
Crear funciones personalizadas.	Crear una función personalizada de vCenter Server
Todos los privilegios y los objetos a los que puede aplicar los privilegios	Capítulo 16 Privilegios definidos
Conjuntos de privilegios que se requieren en diferentes objetos para diferentes tareas.	Privilegios de vCenter Server necesarios para la realización de tareas comunes

El modelo de permisos de los hosts ESXi independientes es más simple. Consulte Asignar privilegios para hosts ESXi.

Qué es la validación de usuarios de vCenter Server

Los sistemas vCenter Server que usan un servicio de directorio suelen validar usuarios y grupos en función del dominio del directorio de usuarios. La validación se produce en intervalos regulares especificados en la configuración de vCenter Server. Por ejemplo, supongamos que al usuario Smith se le asigna una función sobre varios objetos. El administrador de dominios cambia el nombre por Smith2. El host concluye que Smith ya no existe y elimina los permisos asociados con ese usuario de los objetos de vSphere en la siguiente validación.

De modo similar, si se elimina el usuario Smith del dominio, todos los permisos asociados con ese usuario se eliminan en la siguiente validación. Si se agrega un nuevo usuario Smith al dominio antes de la siguiente validación, el nuevo usuario Smith reemplaza al antiguo usuario Smith en los permisos sobre cualquier objeto.

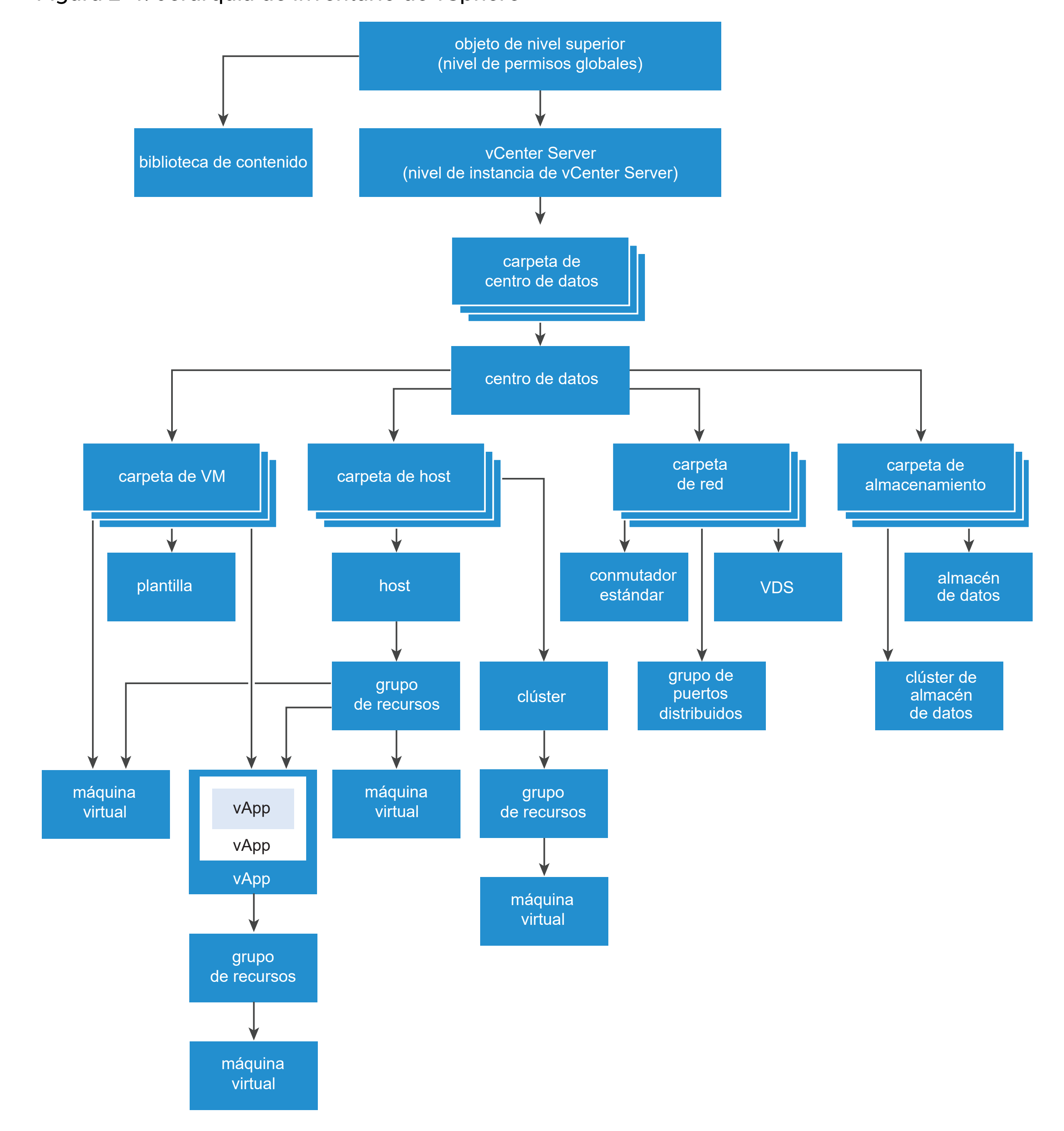
Herencia jerárquica de permisos en vSphere

Al asignar un permiso a un objeto, se puede elegir si el permiso se propagará en la jerarquía de objetos. La propagación se establece para cada permiso. Es decir, no se aplica universalmente. Los permisos definidos para un objeto secundario siempre anulan los permisos propagados desde los objetos primarios.

La siguiente figura ilustra la jerarquía de inventario y las rutas mediante las cuales pueden propagarse los permisos.

Nota Los permisos globales son compatibles con la asignación de privilegios en soluciones de un objeto raíz global. Consulte Usar permisos globales de vCenter Server.

Figura 2-4. Jerarquía de inventario de vSphere



Acerca de esta figura:

- No se pueden establecer permisos directos en las carpetas de máquina virtual, host, red y almacenamiento. Es decir, estas carpetas actúan como contenedores y, por lo tanto, no son visibles para los usuarios.

- No se pueden establecer permisos en conmutadores estándar.

Nota Para poder establecer y propagar permisos en objetos secundarios de un vSphere Distributed Switch (VDS), el objeto del conmutador debe residir en una carpeta de red creada en el centro de datos.

La mayoría de los objetos del inventario heredan permisos de un único objeto primario de la jerarquía. Por ejemplo, el almacén de datos hereda permisos de la carpeta primaria del almacén o del centro de datos primario. Las máquinas virtuales heredan permisos de la carpeta primaria de máquinas virtuales y del host, clúster o grupo de recursos primario simultáneamente.

Por ejemplo, se pueden establecer permisos para un conmutador distribuido y sus grupos de puertos distribuidos asociados si se configuran permisos para un objeto primario, como una carpeta o un centro de datos. También se debe seleccionar la opción para propagar estos permisos a los objetos secundarios.

Los permisos tienen distintas formas en la jerarquía.

Entidades administradas

Las entidades administradas hacen referencia a los siguientes objetos de vSphere. Las entidades administradas ofrecen operaciones específicas que varían según el tipo de entidad. Los usuarios con privilegios pueden definir permisos en entidades administradas. Consulte la documentación vSphere API para obtener más información sobre los objetos, las propiedades y los métodos de vSphere.

- Clústeres
- Centros de datos
- Almacenes de datos
- Clústeres de almacenes de datos
- Carpetas
- Hosts
- Redes (excepto vSphere Distributed Switch)
- Grupos de puertos distribuidos
- Grupos de recursos
- Plantillas
- Máquinas virtuales
- vSphere vApps

Entidades globales

No se pueden modificar los permisos en entidades que derivan sus permisos del sistema vCenter Server raíz.

- Campos personalizados
- Licencias
- Funciones
- Intervalos de estadísticas
- Sesiones

Cómo funciona la configuración de varios permisos en vSphere

Los objetos pueden tener varios permisos, pero solo pueden tener un permiso para cada usuario o grupo. Por ejemplo, un permiso podría especificar que GroupAdmin tiene la función de administrador en un objeto. Otro permiso podría especificar que GroupVMAdmin tiene la función de administrador de máquinas virtuales en el mismo objeto. Sin embargo, el grupo GroupVMAdmin no puede tener otro permiso para el mismo GroupVMAdmin en este objeto.

Un objeto secundario hereda los permisos de su objeto principal si la propiedad de propagación del objeto principal se establece en true. Un permiso que se establece directamente en un objeto secundario reemplaza el permiso en el objeto principal. Consulte Ejemplo 2: permisos secundarios que anulan permisos primarios.

Si se establecen varios permisos grupales en el mismo objeto y un usuario pertenece a dos o más de esos grupos, pueden ocurrir dos situaciones:

- No se han definido permisos para el usuario directamente en el objeto. En ese caso, el usuario obtiene la unión de los permisos que tienen los grupos en ese objeto.
- Se han definido permisos para el usuario directamente en el objeto. En ese caso, los permisos para el usuario tienen prioridad sobre todos los permisos de grupo.

Ejemplo 1: Herencia de permisos de varios grupos

En este ejemplo se muestra cómo un objeto puede heredar varios permisos de los grupos que tienen permisos sobre un objeto primario.

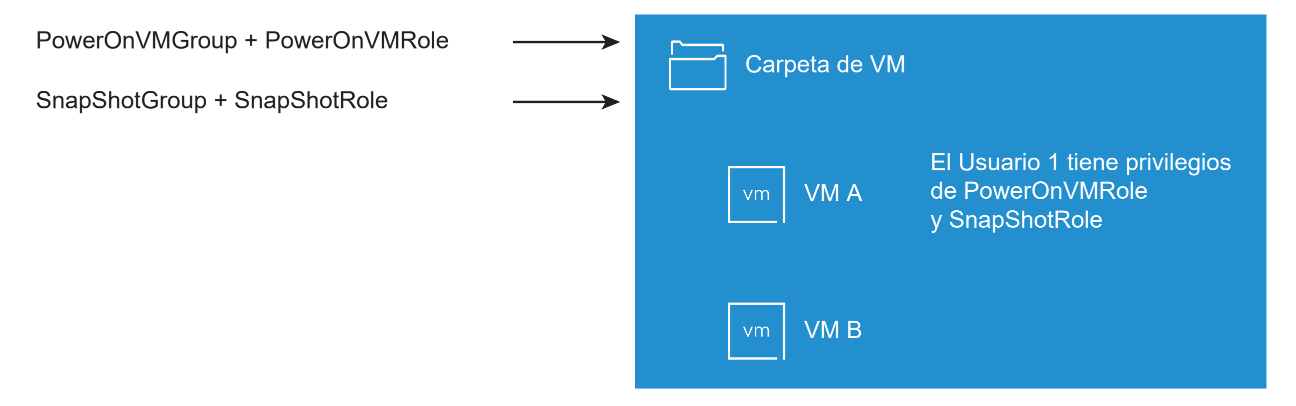
En este ejemplo, se asignan dos permisos sobre el mismo objeto a dos grupos diferentes.

- PowerOnVMRole permite encender las máquinas virtuales.
- SnapShotRole puede crear instantáneas de máquinas virtuales.
- Se asigna PowerOnVMGroup al PowerOnVMRole en la carpeta de máquina virtual; se otorga el permiso para la propagación a objetos secundarios.

- Se asigna SnapShotGroup al SnapShotRole en la carpeta de máquina virtual; se otorga el permiso para la propagación a objetos secundarios.
- No se asignan privilegios específicos al Usuario 1.

El Usuario 1, que pertenece a PowerOnVMGroup y SnapShotGroup, inicia sesión. El Usuario 1 puede encender y crear instantáneas de las máquinas virtuales A y B.

Figura 2-5. Ejemplo 1: Herencia de permisos de varios grupos



Ejemplo 2: permisos secundarios que anulan permisos primarios

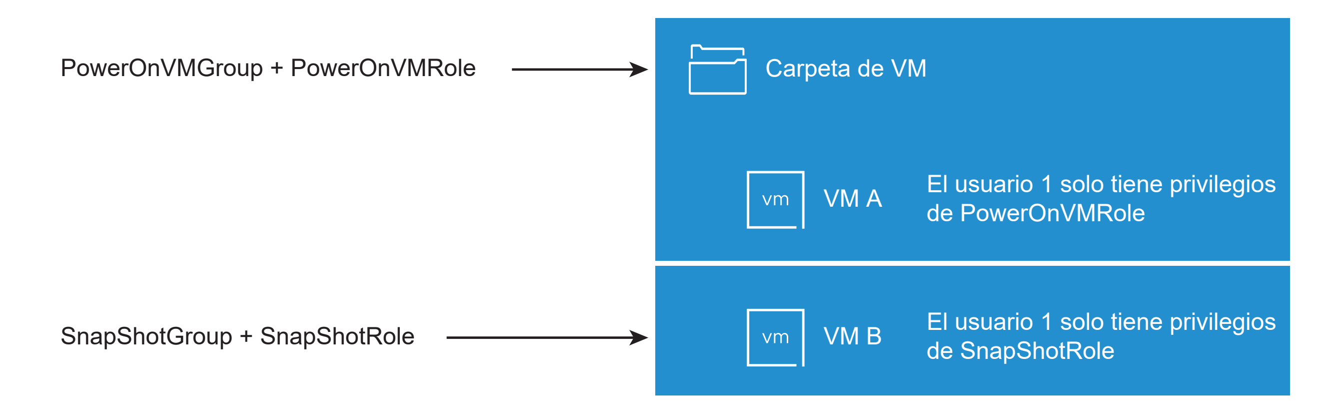
En este ejemplo, se muestra cómo los permisos que se asignan a un objeto secundario pueden anular los permisos que se asignan a un objeto primario. Este comportamiento de anulación se puede utilizar para restringir el acceso de los usuarios a áreas específicas del inventario.

En este ejemplo, los permisos están definidos en dos objetos diferentes de dos grupos distintos.

- PowerOnVMRole permite encender las máquinas virtuales.
- SnapShotRole puede crear instantáneas de máquinas virtuales.
- Se asigna PowerOnVMGroup al PowerOnVMRole en la carpeta de máquina virtual; se otorga el permiso para la propagación a objetos secundarios.
- Se concede SnapShotGroup a SnapShotRole en la máquina virtual B.

El Usuario 1, que pertenece a PowerOnVMGroup y SnapShotGroup, inicia sesión. Ya que SnapShotRole se asigna en un nivel inferior de la jerarquía que PowerOnVMRole, PowerOnVMRole se anula en la máquina virtual B. De esta forma, el Usuario 1 puede encender la máquina virtual A, pero no puede crear instantáneas. El Usuario 1 puede crear instantáneas de la máquina virtual B, pero no puede encenderla.

Figura 2-6. Ejemplo 2: permisos secundarios que anulan permisos primarios



Ejemplo 3: función de usuario que anula la función de grupo

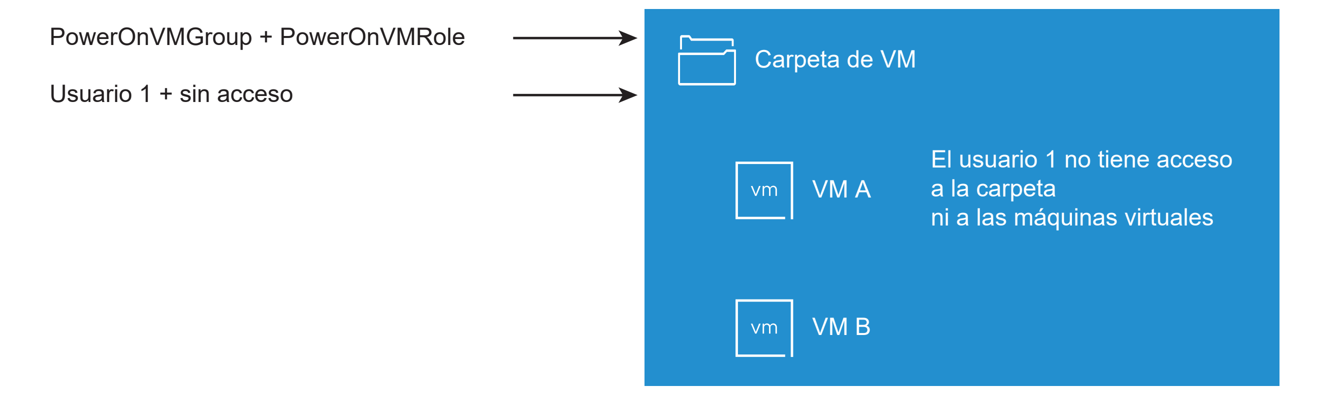
Este ejemplo ilustra cómo la función asignada directamente a un usuario individual anula los privilegios asociados con una función asignada a un grupo.

En este ejemplo, los permisos se definen sobre el mismo objeto. Un permiso asocia un grupo con una función; el otro permiso asocia un usuario individual con una función. El usuario es un miembro del grupo.

- PowerOnVMRole permite encender las máquinas virtuales.
- Se concede PowerOnVMGroup a PowerOnVMRole en la carpeta de máquina virtual.
- Se asigna la función Sin acceso al Usuario 1 en la carpeta de máquina virtual.

El Usuario 1, que pertenece al PowerOnVMGroup, inicia sesión. La función Sin acceso otorgada al Usuario 1 en la carpeta de máquina virtual anula la función asignada al grupo. El Usuario 1 no tiene acceso a la carpeta de máquina virtual o a las máquinas virtuales A y B. Las máquinas virtuales A y B no están visibles en la jerarquía para el Usuario 1.

Figura 2-7. Ejemplo 3: permisos de usuario que anulan permisos de grupo



Administrar permisos para componentes de vCenter Server

Se establece un permiso sobre un objeto en la jerarquía de objetos de vCenter Server. Cada permiso asocia el objeto con un grupo o un usuario y con las funciones de acceso de ese grupo o usuario. Por ejemplo, se puede seleccionar un objeto de la máquina virtual, agregar un permiso que asigne la función de solo lectura al Grupo 1 y, a continuación, agregar un segundo permiso que asigne la función de administrador al Usuario 2.

Al asignar una función diferente a un grupo de usuarios en diferentes objetos, se controlan las tareas que esos usuarios pueden realizar en el entorno de vSphere. Por ejemplo, para permitir que un grupo configure memoria del host, seleccione el host y agregue un permiso que otorgue una función a ese grupo, donde se incluya el privilegio **Host. Configuración.Configuración de memoria**.

Para obtener información conceptual sobre los permisos, consulte el análisis en Descripción del modelo de permisos de nivel de objetos.

Puede asignar permisos sobre objetos de diferentes niveles de la jerarquía; por ejemplo, puede asignar permisos a un objeto del host o una carpeta que incluyan todos los objetos del host. Consulte Herencia jerárquica de permisos en vSphere. Asimismo, puede asignar permisos de propagación a un objeto raíz global donde se apliquen los permisos en todos los objetos de todas las soluciones. Consulte Usar permisos globales de vCenter Server.

Agregar un permiso a un objeto de inventario

Después de crear usuarios y grupos, y definir sus funciones, debe asignarlos a los objetos de inventario correspondientes. Para asignar los mismos permisos de propagación a varios objetos al mismo tiempo, mueva los objetos a una carpeta y configure los permisos allí mismo.

Al asignar permisos, los nombres de los usuarios y los grupos deben coincidir exactamente con los de Active Directory, con distinción de mayúsculas y minúsculas. Si realizó una actualización de versiones anteriores de vSphere y tiene problemas con los grupos, compruebe que no haya inconsistencias de mayúsculas y minúsculas.

Requisitos previos

En el objeto cuyos permisos desea modificar, debe tener una función que incluya el privilegio **Permisos.Modificar permiso**.

Procedimiento

1 Desplácese hasta el objeto para el que desea asignar permisos en el navegador de objetos de vSphere Client.

2 Haga clic en la pestaña **Permisos**.

3 Haga clic en **Agregar**.

4 (opcional) Si configuró un proveedor de identidad externo para autenticación federada, el dominio de dicho proveedor de identidad estará disponible para seleccionarlo en el menú desplegable **Dominio**.

5 Si selecciona **VMware ID** en el menú desplegable **Dominio**, introduzca el nombre de usuario o de grupo.

Nota Introduzca la dirección de correo electrónico de la cuenta de CSP en el campo **Nombre de usuario**. No se pueden buscar cuentas de CSP en el dominio VMwareID.

6 Seleccione el usuario o el grupo que tendrá los privilegios definidos según la función seleccionada.

   a En el menú desplegable **Dominio**, seleccione el dominio para el usuario o el grupo.

   b Escriba un nombre en el cuadro de búsqueda.

      El sistema buscará nombres de usuarios y nombres de grupos.

   c Seleccione el usuario o grupo.

7 Seleccione una función en el menú desplegable **Función**.

8 (opcional) Para propagar los permisos, seleccione la casilla **Propagar a objetos secundarios**.

   La función se aplicará al objeto seleccionado y se propagará a los objetos secundarios.

9 Haga clic en **Aceptar**.

Cambiar o eliminar permisos en un objeto de inventario

Después de que se establece un par usuario/grupo-función para un objeto de inventario, se puede cambiar la función emparejada con el usuario o el grupo, o cambiar la configuración de la casilla **Propagar a objetos secundarios**. También se puede quitar la configuración de permisos.

Procedimiento

1 Desplácese hasta el objeto en el navegador de objetos de vSphere Client.

2 Haga clic en la pestaña **Permisos**.

3 Haga clic en una fila para seleccionar un permiso.

Tarea	Pasos
Cambiar permisos	a Haga clic en **Editar**. b En el menú desplegable **Función**, seleccione una función para el usuario o el grupo. c Active o desactive la casilla **Propagar a objetos secundarios** para cambiar la herencia de permisos. d Haga clic en **Aceptar**.
Quitar permisos	a Haga clic en **Eliminar**. b Haga clic en **Quitar**.

Cambiar la configuración de validación de usuarios de vCenter Server

vCenter Server valida de forma periódica la lista de usuarios y grupos con los usuarios y grupos del directorio de usuarios. A continuación, quita los usuarios y los grupos que ya no existen en el dominio. Se puede desactivar la validación o cambiar el intervalo entre las validaciones. Si tiene dominios con miles de usuarios o grupos, o bien si las búsquedas tardan mucho en completarse, considere ajustar la configuración de la búsqueda.

Esta configuración se aplica a los orígenes de identidad de vCenter Single Sign-On y no a un origen de identidad externo, como Active Directory, que podrían asociarse con vCenter Server.

Nota Este procedimiento se aplica únicamente a las listas de usuarios de vCenter Server. No puede buscar listas de usuarios de ESXi de la misma manera.

Procedimiento

1 Desplácese hasta el sistema vCenter Server en el navegador de objetos de vSphere Client.

2 Seleccione **Configurar** y haga clic en **Configuración > General**.

3 Haga clic en **Editar** y seleccione **Directorio de usuarios**.

4 Cambie los valores según sea necesario y haga clic en **Guardar**.

Opción	Descripción
Tiempo de espera del directorio de usuarios	Intervalo de tiempo de espera, en segundos, para buscar esta instalación de vCenter Server.
Límite de consulta	Active para establecer un número máximo de usuarios y grupos que mostrará vCenter Server.
Tamaño del límite de consulta	Cantidad máxima de usuarios y grupos del dominio seleccionado que vCenter Server muestra en el cuadro de diálogo **Seleccionar usuarios o grupos**. Si escribe 0 (cero), aparecen todos los usuarios y grupos.

Usar permisos globales de vCenter Server

En vCenter Server, los permisos globales se aplican a un objeto raíz global que expande soluciones de VMware. En un SDDC local, los permisos globales pueden abarcar tanto vCenter Server como VMware Aria Automation Orchestrator. Sin embargo, para vSphere SDDC, los permisos globales se aplican a objetos globales, como etiquetas y bibliotecas de contenido.

Puede asignar permisos globales a usuarios o grupos, y decidir qué función asignar a cada usuario o grupo. La función determina el conjunto de privilegios que el usuario o el grupo tienen para todos los objetos de la jerarquía. Puede asignar una función predefinida o crear funciones personalizadas. Consulte Usar funciones de vCenter Server para asignar privilegios.

Es importante distinguir entre los permisos de vCenter Server y los permisos globales.

Tabla 2-1. Diferencias entre permisos de vCenter Server y permisos globales

Tipo de permiso	Descripción
vCenter Server	Los permisos de vCenter Server se aplican a objetos específicos de la jerarquía de inventario, como hosts, máquinas virtuales, almacenes de datos, etc. Cuando se asignan permisos de vCenter Server, se especifica que el usuario o grupo tenga una función (conjunto de privilegios) sobre el objeto.
Global	Los permisos globales conceden a un usuario o grupo privilegios para ver o administrar todos los objetos en cada una de las jerarquías de inventario de la implementación. Los permisos globales también se aplican a objetos globales, como etiquetas y bibliotecas de contenido. Consulte Permisos de vCenter Server en objetos de etiqueta. Si asigna un permiso global y no selecciona Propagar, los usuarios o grupos asociados con este permiso no tendrán acceso a los objetos de la jerarquía. Solo podrán acceder a algunas funcionalidades globales, como la creación de funciones.

Agregar permisos globales

Se pueden utilizar permisos globales para otorgar a un usuario o un grupo privilegios sobre todos los objetos de todas las jerarquías del inventario de la implementación.

Importante Utilice los permisos globales con atención. Compruebe si realmente desea asignar permisos para todos los objetos en todas las jerarquías del inventario.

Requisitos previos

Para realizar esta tarea, se deben tener los privilegios **Permisos.Modificar permisos** en el objeto raíz de todas las jerarquías del inventario.

Procedimiento

1 Inicie sesión en vCenter Server mediante vSphere Client.

2 Seleccione **Administración** y haga clic en **Permisos globales** en el área de control de acceso.

3 Haga clic en **Agregar**.

4 (opcional) Si configuró un proveedor de identidad externo para autenticación federada, el dominio de dicho proveedor de identidad estará disponible para seleccionarlo en el menú desplegable **Dominio**.

5 Para entornos de vSphere+, si selecciona **VMware ID** en el menú desplegable **Dominio**, a continuación tendrá que introducir el nombre de la cuenta de CSP en el campo **Nombre de usuario**.

   Nota Introduzca la dirección de correo electrónico de la cuenta de CSP en el campo **Nombre de usuario**. No se pueden buscar cuentas de CSP en el dominio VMwareID.

6 Seleccione el usuario o el grupo que tendrá los privilegios definidos según la función seleccionada.

   a En el menú desplegable **Dominio**, seleccione el dominio para el usuario o el grupo.

   b Escriba un nombre en el cuadro de búsqueda.

      El sistema buscará nombres de usuarios y nombres de grupos.

   c Seleccione el usuario o grupo.

7 Seleccione una función en el menú desplegable **Función**.

8 Decida si desea propagar los permisos mediante la selección de la casilla **Propagar a objetos secundarios**.

   Si asigna un permiso global y no selecciona **Propagar a objetos secundarios**, los usuarios o grupos asociados con este permiso no tendrán acceso a los objetos de la jerarquía. Solo podrán acceder a algunas funcionalidades globales, como la creación de funciones.

9 Haga clic en **Aceptar**.

Permisos de vCenter Server en objetos de etiqueta

En la jerarquía de objetos de vCenter Server, los objetos de etiqueta no son objetos secundarios de vCenter Server, sino que se crean al nivel superior de vCenter Server. En los entornos que tienen varias instancias de vCenter Server, los objetos de etiqueta se comparten en las instancias de vCenter Server. El funcionamiento de los permisos para los objetos de etiqueta es distinto al de los permisos para otros objetos de la jerarquía de objetos de vCenter Server.

Solo se aplican los permisos globales o los permisos asignados al objeto de etiqueta

Si otorga permisos a un usuario en un objeto de inventario de vCenter Server, como una máquina virtual, ese usuario puede realizar las tareas asociadas con el permiso. Sin embargo, el usuario no puede realizar operaciones de etiquetado en el objeto.

Por ejemplo, si otorga el privilegio **Asignar etiqueta de vSphere** al usuario Dana en el host TPA, ese permiso no afecta la posibilidad de Dana de asignar etiquetas en el host TPA. Dana debe tener el privilegio **Asignar etiqueta de vSphere** en el nivel superior, es decir, un permiso global, o debe tener el privilegio para el objeto de etiqueta.

Tabla 2-2. Cómo influyen los permisos globales y los permisos de objeto de etiqueta en lo que pueden hacer los usuarios

Permiso global	Permiso de nivel de etiqueta	Permiso de nivel de objeto de vCenter Server	Permiso efectivo
No hay privilegios de etiquetado asignados.	Dana tiene los privilegios **Asignar o desasignar etiqueta de vSphere** para la etiqueta.	Dana tiene los privilegios **Eliminar etiqueta de vSphere** en el host ESXi TPA.	Dana tiene los privilegios **Asignar o desasignar etiqueta de vSphere** para la etiqueta.
Dana tiene los privilegios **Asignar o desasignar etiqueta de vSphere**.	No hay privilegios asignados para la etiqueta.	Dana tiene los privilegios **Eliminar etiqueta de vSphere** en el host ESXi TPA.	Dana tiene los privilegios globales **Asignar o desasignar etiqueta de vSphere**. Eso incluye privilegios en el nivel de etiqueta.
No hay privilegios de etiquetado asignados.	No hay privilegios asignados para la etiqueta.	Dana tiene los privilegios **Asignar o desasignar etiqueta de vSphere** en el host ESXi TPA.	Dana no tiene privilegios de etiquetado en ningún objeto, incluido el host TPA.

Los permisos globales complementan los permisos de objeto de etiqueta

Los permisos globales, es decir, los permisos que están asignados en el objeto de nivel superior, complementan los permisos en los objetos de etiqueta cuando los permisos de los objetos de etiqueta tienen más restricciones. Los permisos de vCenter Server no influyen en los objetos de etiqueta.

Por ejemplo, suponga que asigna el privilegio **Eliminar etiqueta de vSphere** al usuario Robin en el nivel superior mediante el uso de permisos globales. Para la producción de la etiqueta, no asigna el privilegio **Eliminar etiqueta de vSphere** a Robin. En ese caso, Robin tiene el privilegio para la producción de etiqueta porque tiene el permiso global, que se propaga desde el nivel superior. No se pueden restringir los privilegios a menos que se modifique el permiso global.

Tabla 2-3. Los permisos globales complementan los permisos de nivel de etiqueta

Permiso global	Permiso de nivel de etiqueta	Permiso efectivo
Robin tiene los privilegios **Eliminar etiqueta de vSphere**.	Robin no tiene los privilegios **Eliminar etiqueta de vSphere** para la etiqueta.	Robin tiene los privilegios **Eliminar etiqueta de vSphere**.
No hay privilegios de etiquetado asignados.	Robin no tiene los privilegios **Eliminar etiqueta de vSphere** asignados para la etiqueta.	Robin no tiene los privilegios **Eliminar etiqueta de vSphere**.

Los permisos de nivel de etiqueta pueden extender los permisos globales

Se pueden utilizar permisos de nivel de etiqueta para extender los permisos globales. Eso significa que los usuarios pueden tener un permiso global y un permiso de nivel de etiqueta en una etiqueta.

Nota Este comportamiento es diferente de la forma vCenter Server se heredan los privilegios. En vCenter Server, los permisos definidos para un objeto secundario siempre anulan los permisos propagados desde los objetos primarios.

Tabla 2-4. Los permisos globales extienden los permisos de nivel de etiqueta

Permiso global	Permiso de nivel de etiqueta	Permiso efectivo
Lee tiene el privilegio **Asignar o desasignar etiqueta de vSphere**.	Lee tiene el privilegio **Eliminar etiqueta de vSphere**.	Lee tiene los privilegios **Asignar etiqueta de vSphere** y **Eliminar etiqueta de vSphere** para la etiqueta.
No hay privilegios de etiquetado asignados.	Lee tiene el privilegio **Eliminar etiqueta de vSphere** asignado para la etiqueta.	Lee tiene el privilegio **Eliminar etiqueta de vSphere** para la etiqueta.

Usar funciones de vCenter Server para asignar privilegios

En vCenter Server, una función es un conjunto predefinido de privilegios que define los derechos para llevar a cabo acciones y propiedades de lectura. Para crear permisos, asigne una función a un usuario o grupo para un objeto. vCenter Server proporciona funciones del sistema y funciones de muestra de forma predeterminada. También puede crear funciones personalizadas.

Asignar permisos en vCenter Server

Al asignar permisos en vCenter Server, se establece un par entre un usuario o grupo y una función, y se asocia ese par a un objeto del inventario. Por ejemplo, puede utilizar la función de muestra de usuario de máquinas virtuales para que los usuarios lean y cambien los atributos de la máquina virtual.

Un solo usuario o grupo puede tener diferentes funciones para distintos objetos del inventario. Por ejemplo, supongamos que tiene dos grupos de recursos en el inventario, el Grupo A y el Grupo B. Puede asignar al grupo Ventas la función de muestra de usuario de la máquina virtual para el Grupo A y la función de solo lectura para el Grupo B. Con estas asignaciones, los usuarios del grupo Ventas pueden encender las máquinas virtuales del Grupo A, pero solo pueden ver las máquinas virtuales del Grupo B.

Los usuarios pueden programar tareas únicamente si tienen una función que incluya privilegios para realizar esa tarea en el momento de crearla.

¿Cuáles son las funciones predefinidas de vCenter Server?

vCenter Server proporciona funciones predefinidas, como se muestra en la tabla siguiente.

Tabla 2-5. Funciones predefinidas de vCenter Server

Tipo de función	Nombres de función	Descripción
Sistema	Administrador, Solo lectura y Sin acceso.	Las funciones del sistema son permanentes. No puede eliminar las funciones del sistema ni editar los privilegios asociados con estas funciones. Las funciones del sistema se organizan como una jerarquía. Cada función hereda los privilegios de la función anterior. Por ejemplo, la función de administrador hereda los privilegios de la función de solo lectura. Consulte la siguiente sección para obtener más información sobre las funciones del sistema.
Ejemplo	vSphere proporciona una serie de funciones de muestra; por ejemplo, AutoUpdateUser, administrador de grupo de recursos y usuario de máquina virtual.	vSphere proporciona funciones de muestra para ciertas combinaciones de tareas frecuentes. Estas funciones se pueden clonar, modificar o quitar. **Nota** Para evitar perder la configuración predefinida en una función de muestra, primero clone la función y, a continuación, realice las modificaciones en el clon. No se puede restablecer la muestra a su configuración predeterminada.

Para ver los privilegios asociados con una función, desplácese hasta esa función en vSphere Client (**Menú > Administración > Funciones**) y haga clic en la pestaña **Privilegios**.

Para ver todos los privilegios y las descripciones de vSphere, consulte Capítulo 16 Privilegios definidos.

Nota Los cambios en las funciones y en los privilegios se aplican de inmediato, incluso si los usuarios involucrados iniciaron sesión. La excepción son las búsquedas, para las cuales los cambios se aplican una vez que el usuario cierra la sesión y vuelve a iniciarla.

Funciones del sistema vCenter Server

Las funciones del sistema no se pueden modificar ni eliminar.

Función de administrador

Los usuarios con la función de administrador para un objeto tienen permiso de ver el objeto y realizar todas las acciones posibles en él. Esta función también incluye todos los privilegios inherentes a la función de solo lectura. Si tiene la función de administrador en un objeto, puede asignar privilegios a grupos y usuarios individuales.

Si actúa con función de administrador en vCenter Server, puede asignar privilegios a los usuarios y grupos del origen de identidad predeterminado de vCenter Single Sign-On.

Consulte la documentación de *vSphere Authentication* para obtener información sobre los servicios de identidad admitidos.

De forma predeterminada, el usuario administrator@vsphere.local tiene la función de administrador tanto en vCenter Single Sign-On como en vCenter Server después de la instalación. Ese usuario puede asociar otros usuarios con la función de administrador en vCenter Server.

Sugerencia La práctica recomendada es crear un usuario en el nivel raíz y asignar la función Administrador a ese usuario. Después de crear un usuario designado con privilegios de Administrador, puede quitar el usuario raíz de cualquiera de los permisos o cambiar la función a Sin acceso.

Función de solo lectura

Los usuarios con la función Solo lectura para un objeto tienen permiso de ver el estado y los detalles del objeto. Por ejemplo, los usuarios con esta función pueden ver atributos de máquinas virtuales, hosts y grupos de recursos, pero no pueden ver la consola remota para un host. Las acciones desde los menús y las barras de herramientas no están permitidas.

Función Sin acceso

Los usuarios con la función Sin acceso a un objeto no pueden ver ni cambiar ese objeto de ninguna manera. Los usuarios y grupos nuevos tienen asignada esta función de forma predeterminada. Es posible cambiar la función de un solo objeto a la vez.

El administrador del dominio de vCenter Single Sign-On, administrator@vsphere.local de manera predeterminada, el usuario raíz y vpxuser tienen asignada la función Administrador de manera predeterminada. De manera predeterminada, se asigna la función Sin acceso a los otros usuarios.

Funciones personalizadas en vCenter Server y ESXi

Se pueden crear funciones personalizadas para vCenter Server y todos los objetos que administra, o bien para hosts individuales.

Funciones personalizadas de vCenter Server (recomendado)

Si se desean crear funciones personalizadas, se pueden utilizar las opciones de edición de funciones en vSphere Client para crear conjuntos de privilegios que se adapten a los requisitos.

Funciones personalizadas de ESXi

Se pueden crear funciones personalizadas para hosts individuales mediante la utilización de una CLI o de VMware Host Client. Consulte la documentación de *Administrar un host único de vSphere: VMware Host Client*. No se puede acceder a las funciones de host personalizadas desde vCenter Server.

Si administra los hosts ESXi mediante vCenter Server, no mantenga las funciones personalizadas en el host y en vCenter Server. Defina las funciones en el nivel de vCenter Server.

Cuando se administra un host por medio de vCenter Server, los permisos asociados con ese host se crean desde vCenter Server y se almacenan en vCenter Server. Si se conecta directamente a un host, solo están disponibles las funciones que se crearon de forma directa en el host.

Nota Cuando se agrega una función personalizada y no se le asignan privilegios, la función creada es de solo lectura con tres privilegios definidos por el sistema: **Sistema.Anónimo**, **Sistema.Ver** y **Sistema.Leer**. Estos privilegios no están visibles en vSphere Client, pero se utilizan para leer ciertas propiedades de algunos objetos administrados. Todas las funciones predefinidas en vCenter Server contienen estos tres privilegios definidos por el sistema. Consulte la documentación sobre *vSphere Web Services API* para obtener más información.

Crear una función personalizada de vCenter Server

Para adaptarse a las necesidades de control de acceso de su entorno, puede crear funciones personalizadas de vCenter Server. Puede crear una función o clonar una función existente.

Puede crear o editar una función en un sistema vCenter Server que forme parte del mismo dominio de vCenter Single Sign-On que los otros sistemas vCenter Server. VMware Directory Service (vmdir) propaga los cambios que se realicen en la función a todos los demás sistemas vCenter Server en el grupo. Las asignaciones de funciones a usuarios y objetos específicos no se comparten en los sistemas vCenter Server.

Requisitos previos

Compruebe que tenga privilegios de administrador en el sistema vCenter Server en el que cree la función.

Procedimiento

1 Inicie sesión en vCenter Server mediante vSphere Client.

2 Seleccione **Administración** y haga clic en **Funciones** en el área **Control de acceso**.

3 Cree la función.

Opción	Descripción
Para crear una función	a Haga clic en **Nueva**. b Escriba un nombre para la nueva función. c Seleccione privilegios para la función o anule la selección de estos. Desplácese por las categorías de privilegios y seleccione todos los privilegios o un subconjunto de privilegios para esa categoría. Puede mostrar todas las categorías, seleccionadas o sin seleccionar. También puede mostrar todos los privilegios, seleccionados o sin seleccionar. Consulte Capítulo 16 Privilegios definidos para obtener más información. d Haga clic en **Crear**.
Para crear la función mediante clonación	a Seleccione una función y haga clic en **Clonar**. b Introduzca un nombre para la función. c Haga clic en **Aceptar**. **Nota** Cuando se crea una función clonada, no se pueden cambiar los privilegios. Para cambiar los privilegios, seleccione la función clonada y haga clic en **Editar**.

Pasos siguientes

Ahora puede crear permisos mediante la selección de un objeto y la asignación de la función a un usuario o un grupo para dicho objeto.

Usar registrador de privilegios

En vSphere, los privilegios son controles de acceso detallados que se pueden agrupar en funciones y asignarse a usuarios o grupos. El registrador de privilegios le ayuda a identificar el conjunto mínimo de privilegios necesarios para ejecutar un flujo de trabajo de vCenter Server.

Para ejecutar un conjunto específico de operaciones, es muy difícil determinar el conjunto mínimo de privilegios que requiere el usuario. Los privilegios no tienen una correspondencia de uno a uno con el flujo de trabajo específico, que generalmente consta de varias llamadas a diferentes API que funcionan en el objeto correspondiente. Como resultado, el usuario tiene más acceso o muy poco acceso al entorno. Con el objetivo de mantener protegido el entorno, la función de registrador de privilegios ayuda a identificar el conjunto mínimo de privilegios necesario para ejecutar un flujo de trabajo de vCenter Server. Permite supervisar y consultar los privilegios que se comprobaron al realizar una operación. El registrador de privilegios se implementa mediante un REST API.

Nota Esta función está disponible como API y solo admite flujos de trabajo que se ejecutan mediante un script. No hay compatibilidad con la interfaz de usuario para el registrador de privilegios.

Una consulta a ListAPI permite recuperar listas de comprobaciones de privilegios junto con las sesiones, los usuarios, los objetos administrados y los identificadores de operación (opID) correspondientes. Puede utilizar los filtros adecuados para obtener privilegios para un flujo de trabajo en particular.

Por ejemplo, supongamos que el usuario A necesita crear una máquina virtual. La creación de una máquina virtual requiere un determinado conjunto de privilegios. El usuario A debe solicitar privilegios al administrador del sistema. El administrador del sistema puede habilitar el registrador de privilegios y ejecutar la operación de creación de la máquina virtual. Mientras se realiza la comprobación de privilegios, se almacenan los datos de los privilegios que se comprobaron durante la operación Crear máquina virtual. Los datos contienen PrivilegeID, sessionID, OpID, etc. En este ejemplo, este administrador del sistema utilizará los filtros para obtener privilegios para el flujo de trabajo de creación de la máquina virtual. El administrador del sistema ahora puede crear una función con los privilegios mínimos necesarios y asignarla al usuario.

Habilitar el registrador de privilegios

Para habilitar el registrador de privilegios, utilice vSphere Client para modificar el archivo de configuración de vCenter Server: `vpxd.cfg`.

Requisitos previos

Compruebe que dispone de privilegios suficientes para ejecutar el flujo de trabajo. Se recomienda un usuario con la función de administrador.

Procedimiento

1 Inicie sesión en vCenter Server mediante vSphere Client.

2 Acceda a la instancia de vCenter Server.

3 Seleccione **Configurar > Configuración avanzada**.

4 Haga clic en **Editar configuración**.

5 Agregue la configuración.

   Desplácese hacia abajo y, en el campo **Nombre**, introduzca el nombre de la opción y, en el campo **Valor**, introduzca el valor de la configuración especificada.

Configuración	Descripción
config.vpxd.privCheck.bufferSize	El recuento de privilegios que se conservarán en la memoria. El valor predeterminado es 0. Si no cambia el valor predeterminado, el registrador de comprobaciones de privilegios no registra ningún dato.
config.vpxd.privCheck.cleanupInterval	El intervalo en el que se limpian las comprobaciones de privilegios de las sesiones sin utilizar. El valor predeterminado es 30 minutos.

6 Haga clic en **Agregar** y **Guardar**.

Pasos siguientes

Consulte Realizar operaciones de comprobaciones de privilegios en la *Guía de programación de VMware vSphere Automation SDK*.

Prácticas recomendadas para funciones y permisos de vCenter Server

Siga las prácticas recomendadas para funciones y permisos a fin de maximizar la seguridad y la facilidad de administración del entorno de vCenter Server.

Siga estas prácticas recomendadas para configurar funciones y permisos en un entorno de vCenter Server:

- Siempre que sea posible, asigne una función a un grupo en lugar de hacerlo a usuarios individuales.
- Otorgue permisos solo en los objetos en los que esto sea necesario y asigne privilegios solo a los usuarios o grupos que deban tenerlos. Use la cantidad mínima de permisos para facilitar la comprensión y la administración de la estructura de permisos.
- Si asigna una función restrictiva a un grupo, compruebe que el grupo no contenga el usuario administrador u otros usuarios con privilegios administrativos. De lo contrario, podría restringir los privilegios de administradores de forma accidental en partes de la jerarquía de inventario en las que asignó la función restrictiva al grupo.
- Agrupe los objetos en carpetas para que sea más fácil asignar permisos. Por ejemplo, para conceder el permiso de modificación para un grupo de hosts y el permiso de visualización para otro conjunto de hosts, coloque cada conjunto de hosts en una carpeta.
- Tenga cuidado al agregar un permiso a los objetos raíz de vCenter Server. Los usuarios con privilegios en nivel de raíz tienen acceso a los datos globales en vCenter Server, como funciones, atributos personalizados y configuración de vCenter Server.
- Considere la posibilidad de habilitar la propagación al asignar los permisos a un objeto. La propagación garantiza que los objetos nuevos de la jerarquía de objetos hereden los permisos. Por ejemplo, puede asignar un permiso a una carpeta de máquina virtual y habilitar la propagación para garantizar que el permiso se aplique a todas las máquinas virtuales de la carpeta.
- Utilice la función Sin acceso para enmascarar determinadas áreas de la jerarquía. La función Sin acceso restringe el acceso a los usuarios o grupos que tengan esa función. Sin embargo, en el caso de las máquinas virtuales y las VMware® vApp, existen dos cadenas de propagación de permisos. La asignación de un permiso de propagación con la función Sin acceso en una de las cadenas no implica que la vApp o la máquina virtual respectivas no tengan privilegios propagados en ellas.
- Los cambios en las licencias se propagan a todos los sistemas vCenter Server vinculados en el mismo dominio de vCenter Single Sign-On.

- La propagación de las licencias se produce incluso si el usuario no tiene privilegios en todos los sistemas vCenter Server.

Privilegios de vCenter Server necesarios para la realización de tareas comunes

Muchas tareas necesitan permisos en varios objetos del inventario de vSphere. Si el usuario que intenta realizar la tarea únicamente tiene privilegios en un solo objeto, la tarea no se puede completar de forma correcta.

En la siguiente tabla, se enumeran las tareas comunes que necesitan más de un privilegio. Puede agregar permisos a los objetos del inventario mediante el emparejamiento de un usuario con una de las funciones predefinidas o con varios privilegios. Si prevé que tendrá que asignar un conjunto de privilegios varias veces, cree funciones personalizadas. Para obtener más información sobre los privilegios necesarios para tareas comunes, consulte Usar registrador de privilegios.

Consulte la documentación de referencia de la API de *vSphere Web Services* para obtener información sobre cómo se asignan las operaciones de la interfaz de usuario de vSphere Client a las llamadas API y los privilegios necesarios para realizar operaciones. Por ejemplo, la documentación de la API del método `AddHost_Task(addHost)` especifica que se requiere el privilegio Host.Inventory.AddHostToCluster para agregar un host a un clúster.

Si la tarea que desea realizar no figura en la tabla, las siguientes reglas explican dónde debe asignar permisos para permitir determinadas operaciones:

- Cualquier operación que consume espacio de almacenamiento requiere el privilegio **Almacén de datos.Asignar espacio** en el almacén de datos de destino, así como el privilegio para realizar la operación en sí. Debe tener estos privilegios, por ejemplo, cuando se crea un disco virtual o toma una instantánea.
- Mover un objeto en la jerarquía del inventario requiere los privilegios apropiados en el objeto mismo, el objeto primario de origen (como una carpeta o un clúster) y el objeto primario de destino.
- Cada host o clúster tiene su propio grupo de recursos implícito, que contiene todos los recursos de ese host o clúster. Para implementar una máquina virtual directamente en un host o un clúster, se necesita el privilegio **Recurso.Asignar máquina virtual a un grupo de recursos**.

Tabla 2-6. Privilegios necesarios para la realización de tareas comunes

Tarea	Privilegios necesarios	Función aplicable
Crear una máquina virtual	En la carpeta de destino o el centro de datos: ■ **Máquina virtual.Editar el inventario.Crear nuevo** ■ **Máquina virtual.Cambiar configuración.Agregar disco nuevo** (si se está creando un nuevo disco virtual) ■ **Máquina virtual.Cambiar configuración.Agregar un disco existente** (si se está usando un disco virtual existente) ■ **Máquina virtual.Configuración.Configurar dispositivo sin formato** (si se está usando un dispositivo de acceso directo RDM o SCSI)	Administrador
	En el host, clúster o grupo de recursos de destino: **Recurso.Asignar máquina virtual a grupo de recursos**	Administrador del grupo de recursos o Administrador
	En el almacén de datos de destino o la carpeta que contiene el almacén de datos: **Almacén de datos.Asignar espacio**	Administrador o Consumidor del almacén de datos
	En la red a la cual se asignará la máquina virtual: **Red.Asignar red**	Administrador o Consumidor de la red
Encender una máquina virtual	En el centro de datos en el que se implementa la máquina virtual: **Virtual machine.Interaction.Power On**	Administrador o Usuario avanzado de la máquina virtual
	En la máquina virtual o en una carpeta de máquinas virtuales: **Virtual machine.Interaction.Power On**	
Implementación de una máquina virtual desde una plantilla	En la carpeta de destino o el centro de datos: ■ **Máquina virtual.Editar el inventario.Crear a partir de existente** ■ **Máquina virtual.Cambiar configuración.Agregar disco nuevo**	Administrador
	En una plantilla o una carpeta de plantillas: **Virtual machine.Provisioning.Deploy template**	Administrador
	En el host, clúster o grupo de recursos de destino: ■ **Recurso.Asignar máquina virtual a grupo de recursos** ■ **vApp.Importar**	Administrador
	En el almacén de datos de destino o en la carpeta de almacenes de datos: **Almacén de datos.Asignar espacio**	Administrador o Consumidor del almacén de datos
	En la red a la cual se asignará la máquina virtual: **Red.Asignar red**	Administrador o Consumidor de la red
Creación de una snapshot de una máquina virtual	En la máquina virtual o en una carpeta de máquinas virtuales: **Máquina virtual.Administración de instantáneas.Crear instantánea**	Administrador o Usuario avanzado de la máquina virtual

Tabla 2-6. Privilegios necesarios para la realización de tareas comunes (continuación)

Tarea	Privilegios necesarios	Función aplicable
Transferencia de una máquina virtual a un grupo de recursos	En la máquina virtual o en una carpeta de máquinas virtuales: ■ **Recurso.Asignar máquina virtual a grupo de recursos** ■ **Máquina virtual.Editar el inventario.Mover**	Administrador
	En el grupo de recursos de destino: **Recurso.Asignar máquina virtual a grupo de recursos**	Administrador
Instalar un sistema operativo invitado en una máquina virtual	En la máquina virtual o en una carpeta de máquinas virtuales: ■ **Virtual machine.Interaction.Answer question** ■ **Virtual machine.Interaction.Console interaction** ■ **Virtual machine.Interaction.Device connection** ■ **Virtual machine.Interaction.Power Off** ■ **Virtual machine.Interaction.Power On** ■ **Virtual machine.Interaction.Reset** ■ **Máquina virtual .Interacción.Configurar medio de CD** (si se está instalando desde un CD) ■ **Máquina virtual .Interacción.Configurar medio de disquete** (si se está instalando desde un disquete) ■ **Virtual machine.Interaction.VMware Tools install**	Administrador o Usuario avanzado de la máquina virtual
	En un almacén de datos que contiene la imagen ISO de los medios de instalación: **Almacén de datos.Examinar almacén de datos** (si se está instalando desde una imagen ISO en un almacén de datos) En el almacén de datos en el que se cargue la imagen ISO de los medios de instalación: ■ **Almacén de datos.Examinar almacén de datos** ■ **Almacén de datos.Operaciones de archivos de bajo nivel**	Administrador o Usuario avanzado de la máquina virtual
Migración de una máquina virtual con vMotion	En la máquina virtual o en una carpeta de máquinas virtuales: ■ **Recurso.Migrar máquina virtual encendida** ■ **Recurso.Asignar máquina virtual a un grupo de recursos** (si el destino es un grupo de recursos distinto al de origen)	Administrador del grupo de recursos o Administrador
	En el host, clúster o grupo de recursos de destino (si es distinto al de origen): **Recurso.Asignar máquina virtual a grupo de recursos**	Administrador del grupo de recursos o Administrador
Migración en frío (reubicación) de una máquina virtual	En la máquina virtual o en una carpeta de máquinas virtuales: ■ **Recurso.Migrar máquina virtual apagada** ■ **Recurso.Asignar máquina virtual a grupo de recursos** (si el destino es un grupo de recursos distinto al de origen)	Administrador del grupo de recursos o Administrador
	En el host, clúster o grupo de recursos de destino (si es distinto al de origen): **Recurso.Asignar máquina virtual a grupo de recursos**	Administrador del grupo de recursos o Administrador

Tabla 2-6. Privilegios necesarios para la realización de tareas comunes (continuación)

Tarea	Privilegios necesarios	Función aplicable
	En el almacén de datos de destino (si es distinto al de origen): **Almacén de datos.Asignar espacio**	Administrador o Consumidor del almacén de datos
Migración de una máquina virtual con Storage vMotion	En la máquina virtual o en una carpeta de máquinas virtuales: **Recurso.Migrar máquina virtual encendida**	Administrador del grupo de recursos o Administrador
	En el almacén de datos de destino: **Almacén de datos.Asignar espacio**	Administrador o Consumidor del almacén de datos
Transferencia de un host a un clúster	En el host: **Host.Inventario.Agregar host a clúster**	Administrador
	En el clúster de destino: ■ **Host.Inventario.Agregar host a clúster** ■ **Host.Inventario.Modificar clúster**	Administrador
Agregar un solo host a un centro de datos mediante vSphere Client o agregar un solo host a un clúster mediante PowerCLI o la API (aprovechando la API de addHost)	En el host: **Host.Inventario.Agregar host a clúster**	Administrador
	En el clúster: ■ **Host.Inventario.Modificar clúster** ■ **Host.Inventario.Agregar host a clúster**	Administrador
	En el centro de datos: **Host.Inventario.Agregar host independiente**	Administrador
Agregar varios hosts a un clúster	En el clúster: ■ **Host.Inventario.Modificar clúster** ■ **Host.Inventario.Agregar host a clúster**	Administrador
	En el centro de datos principal del clúster (con propagación): ■ **Host.Inventario.Agregar host independiente** ■ **Host.Inventario.Mover host** ■ **Host.Inventario.Modificar clúster** ■ **Host.Configuración.Mantenimiento**	Administrador
Cifrado de una máquina virtual	Las tareas de cifrado son solo posibles en los entornos que incluyen vCenter Server. Además, el host ESXi debe tener un modo de cifrado habilitado para la mayoría de las tareas de cifrado. El usuario que realiza la tarea debe contar con los privilegios correspondientes. Un conjunto de privilegios **Operaciones criptográficas** permite un control detallado. Consulte Requisitos previos y privilegios necesarios para tareas de cifrado de máquinas virtuales.	Administrador
Proteger una máquina virtual (si utiliza vSphere+ para protegerla)	En el centro de datos en el que se implementa la máquina virtual: ■ **Etiquetado de vSphere.Asignar o desasignar etiqueta de vSphere**	Administrador

Proteger hosts ESXi

3

La arquitectura del hipervisor de ESXi tiene muchas características de seguridad incorporadas, como aislamiento de la CPU, aislamiento de la memoria y aislamiento del dispositivo. Es posible configurar características como el modo de bloqueo, el reemplazo de certificados y la autenticación de tarjeta inteligente para una seguridad mejorada.

Un host ESXi también está protegido con un firewall. Puede abrir los puertos para el tráfico entrante y saliente según sea necesario, pero debe restringir el acceso a los servicios y los puertos. El modo de bloqueo de ESXi y la limitación de acceso a ESXi Shell puede contribuir aún más a un entorno más seguro. Los hosts ESXi participan en la infraestructura de certificados. Los hosts están aprovisionados con certificados firmados por VMware Certificate Authority (VMCA) de forma predeterminada.

Consulte el informe técnico VMware *Seguridad de VMware vSphere Hypervisor* para obtener información adicional sobre la seguridad de ESXi.

Nota ESXi no se basa en el kernel de Linux ni en una distribución convencional de Linux. Utiliza sus propias herramientas de software y kernel especializadas de VMware, que se proporcionan como una unidad independiente, y no contiene aplicaciones ni componentes de las distribuciones de Linux.

A partir de vSphere 8.0 Update 1, ESXi ejecuta dos servicios de proxy inverso:

- El servicio de proxy inverso de VMware, `rhttpproxy`
- Envoy

Envoy tiene el puerto 443 y todas las solicitudes entrantes de ESXi se enrutan mediante Envoy. A partir de vSphere 8.0 Update 1, rhttpproxy funciona como un servidor de administración de configuración para Envoy.

Lea los siguientes temas a continuación:

Recomendaciones generales sobre seguridad de ESXi

Para proteger un host ESXi contra la intromisión no autorizada o el uso incorrecto, VMware impone restricciones sobre varios parámetros, opciones de configuración y actividades. Para satisfacer sus necesidades de configuración, puede modificar las restricciones. Si lo hace, asegúrese de trabajar en un entorno de confianza y tome otras medidas de seguridad.

Cuáles son las funciones de seguridad integradas de ESXi

ESXi mitiga los riesgos para los hosts de la siguiente manera:

- La interfaz de ESXi Shell y la interfaz SSH están desactivadas de forma predeterminada. Mantenga estas interfaces desactivadas a menos que esté realizando actividades de solución de problemas o de soporte. Para las actividades cotidianas, utilice la vSphere Client, donde la actividad está sujeta al control de acceso basado en roles y a métodos de control de acceso modernos.
- Solo algunos puertos de firewall están abiertos de forma predeterminada. Puede abrir de forma explícita puertos de firewall asociados con dispositivos específicos.
- De forma predeterminada, todos los puertos que no son necesarios para el acceso de administración al host están cerrados. Abra los puertos si necesita servicios adicionales.
- ESXi ejecuta solo los servicios que son fundamentales para administrar sus funciones. La distribución está limitada a las características necesarias para ejecutar ESXi.
- De forma predeterminada, los cifrados débiles están desactivados y las comunicaciones de los clientes están protegidas con SSL. Los algoritmos exactos utilizados para proteger el canal dependen del protocolo de enlace de SSL. Los certificados predeterminados creados en ESXi utilizan el cifrado PKCS#1 SHA-256 con RSA como algoritmo de firmas.

- ESXi utiliza un servicio web interno para permitir el acceso a través de clientes web. El servicio se modificó para que ejecute solo las funciones que necesita un cliente web para la administración y la supervisión. Por lo tanto, ESXi no es vulnerable a los problemas de seguridad del servicio web que se experimentan durante el uso general.
- VMware supervisa todas las alertas de seguridad que pueden afectar la seguridad de ESXi y emite una revisión de seguridad según sea necesario. Para recibir alertas de seguridad, puede suscribirse a la lista de correo de advertencias y alertas de seguridad de VMware. Consulte la página web en http://lists.vmware.com/mailman/listinfo/security-announce.
- No se instalan servicios no seguros, como FTP y Telnet, y sus puertos están cerrados de forma predeterminada.
- Para proteger a los hosts de la carga de controladores y aplicaciones que no están firmados criptográficamente, utilice el arranque seguro UEFI. La habilitación del arranque seguro se realiza en el BIOS del sistema. No se requieren cambios de configuración adicionales en el host ESXi, por ejemplo, para las particiones de disco. Consulte Arranque seguro UEFI para hosts ESXi.
- Si el host ESXi tiene un chip TPM 2.0, habilite y configure el chip en el BIOS del sistema. Al trabajar junto con el arranque seguro, TPM 2.0 proporciona una seguridad mejorada y una garantía de confianza basada en hardware. Consulte Proteger hosts ESXi con el módulo de plataforma de confianza.
- En ESXi 8.0 y versiones posteriores, puede ejecutar el proceso de SSH en un dominio de espacio aislado. A continuación, el shell tiene privilegios reducidos y solo permite el acceso a un subconjunto limitado de comandos. Para obtener más información, consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/87386.

Tomar otras medidas de seguridad de ESXi

Tenga en cuenta las siguientes recomendaciones al evaluar la seguridad y la administración de los hosts.

Limitar el acceso a hosts ESXi

Si activa el acceso a la interfaz de usuario de la consola directa (Direct Console User Interface, DCUI), a ESXi Shell o a SSH, aplique directivas de seguridad de acceso estrictas.

ESXi Shell tiene acceso privilegiado a ciertas partes del host. Proporcione acceso de inicio de sesión a ESXi Shell solo a usuarios de confianza.

No acceda a los hosts ESXi administrados directamente

Utilice vSphere Client para administrar los hosts ESXi que administra un sistema vCenter Server. No acceda directamente a los hosts administrados con VMware Host Client y no cambie los hosts administrados de la DCUI.

Si administra hosts con una interfaz o API de scripting, no apunte directamente al host. En su lugar, apunte al sistema vCenter Server que administra el host y especifique el nombre de host.

Usar la DCUI solamente para la solución de problemas

Acceda al host desde la DCUI o ESXi Shell como usuario raíz solo para solucionar problemas. Para administrar los hosts ESXi, utilice vSphere Client (o VMware Host Client) o una de las CLI o las API de VMware. Consulte *Conceptos y ejemplos de ESXCLI*. Si utiliza ESXi Shell o SSH, limite las cuentas que tienen acceso y establezca tiempos de espera.

Usar orígenes de VMware solamente para actualizar los componentes de ESXi

El host ejecuta varios paquetes externos para admitir las interfaces de administración o las tareas que se deben realizar. VMware solo admite actualizaciones para estos paquetes que provienen de un origen de VMware. Si utiliza una descarga o una revisión de otro origen, puede comprometer la seguridad o las funciones de la interfaz de administración. Compruebe los sitios de proveedores externos y la base de conocimientos de VMware para consultar las alertas de seguridad.

Nota Siga los avisos de seguridad de VMware en http://www.vmware.com/security/.

Configuración avanzada del sistema ESXi

La configuración avanzada del sistema controla aspectos del comportamiento ESXi, como el registro, los recursos del sistema y la seguridad.

En la siguiente tabla, se presentan algunas de las opciones avanzadas importantes para seguridad del sistema ESXi. Para ver toda la configuración avanzada del sistema, consulte vSphere Client (**Host > Configurar > Sistema > Configuración avanzada del sistema)** o la API para una versión determinada.

Tabla 3-1. Lista parcial de la configuración avanzada del sistema de seguridad

Configuración avanzada del sistema	Descripción	Valor predeterminado
Annotations.WelcomeMessage	Muestra un mensaje de bienvenida en Host Client antes de iniciar sesión o en la interfaz de usuario de la consola directa (Direct Console User Interface, DCUI) en la pantalla predeterminada. En la DCUI, el mensaje de bienvenida reemplaza a algún texto, como la dirección IP del host.	(Vacío)
Config.Etc.issue	Muestra un banner durante una sesión de inicio de sesión SSH.	(Vacío)

Tabla 3-1. Lista parcial de la configuración avanzada del sistema de seguridad (continuación)

Configuración avanzada del sistema	Descripción	Valor predeterminado
Config.Etc.motd	Muestra el mensaje del día al iniciar sesión en SSH. **Nota** Para insertar nuevas líneas o retornos en los problemas y las configuraciones de motd, puede utilizar tanto vSphere API como la CLI. Por ejemplo, consulte https://williamlam.com/2021/03/adding-a-customized-notification-banner-in-the-vsphere-ui.html y https://williamlam.com/2015/02/easily-manage-esxi-vcsa-ssh-login-banner-motd-in-vsphere-6-0.html.	(Vacío)
Config.HostAgent.vmacore.soap.sessionTimeout	Establece el tiempo de inactividad en minutos antes de que el sistema cierre sesión automáticamente en una API de VIM. El valor 0 (cero) desactiva el tiempo de inactividad. Esta opción solo se aplica a las nuevas sesiones.	30 (minutos)
Mem.MemEagerZero	Activa la aplicación a cero del ámbito del usuario y las páginas de memoria del invitado en los sistemas operativos VMkernel (incluido el proceso VMM) después de que se cierra una máquina virtual. El valor predeterminado (0) utiliza la puesta a cero lenta. El valor 1 utiliza la puesta a cero rápida.	0 (desactivado)

Tabla 3-1. Lista parcial de la configuración avanzada del sistema de seguridad (continuación)

Configuración avanzada del sistema	Descripción	Valor predeterminado
Security.AccountLockFailures	Establece el número máximo de intentos de inicio de sesión fallidos antes de que el sistema bloquee la cuenta de un usuario. Por ejemplo, para bloquear la cuenta en el quinto error de inicio de sesión, establezca este valor en 4. El valor 0 (cero) desactiva el bloqueo de cuentas. Por motivos de implementación, algunos mecanismos de inicio de sesión cuentan de forma inesperada: ■ Los inicios de sesión de VIM (incluido lVMware Host Client) y ESXCLI reflejan el número exacto de inicios de sesión fallidos. ■ Las conexiones SSH cuentan como intentos de inicio de sesión cuando se muestra una solicitud de contraseña y anulan dicho recuento al iniciar sesión correctamente. Este comportamiento es normal para las comunicaciones de desafío y respuesta. ■ Los inicios de sesión de CGI cuentan con un recuento doble los errores de inicio de sesión. **Precaución** Debido a este problema, un usuario puede bloquearse más rápido que el número de inicios de sesión fallidos cuando se utiliza la interfaz de CGI.	5
Security.AccountUnlockTime	Establece la cantidad de segundos en los que un usuario queda bloqueado. Cualquier intento de inicio de sesión dentro del tiempo de espera de bloqueo especificado reinicia el tiempo de espera de bloqueo.	900 (15 minutos)

Tabla 3-1. Lista parcial de la configuración avanzada del sistema de seguridad (continuación)

Configuración avanzada del sistema	Descripción	Valor predeterminado
Security.PasswordHistory	Establece el número de contraseñas que se deben recordar para cada usuario. Esta opción evita contraseñas duplicadas o similares.	5
Security.PasswordMaxDays	Establece el número máximo de días entre cambios de contraseña.	99999
Security.PasswordQualityControl	Cambia la longitud requerida y el requisito de clase de caracteres, o permite frases de contraseña en la configuración de `Pam_passwdqc`. Puede utilizar caracteres especiales en las contraseñas. Puede tener una longitud de contraseña de al menos 15 caracteres. La configuración predeterminada requiere tres clases de caracteres y una longitud mínima de siete caracteres. Si implementa el anexo de DoD, puede combinar la opción de `similar=deny` más una longitud mínima de contraseña para exigir que las contraseñas sean lo suficientemente diferentes. La configuración del historial de contraseñas solo se aplica para las contraseñas cambiadas a través de la API de `LocalAccountManager.changePassword` de VIM. Para cambiar la contraseña, es necesario que el usuario tenga permiso de administrador. La opción PasswordQualityControl, con una opción PasswordMaxDays, satisface los requisitos del anexo de DoD: `min=disabled,disabled,disabled,disabled,15 similar=deny`	retry=3 min=disabled,disabled,disabled,7,7

Tabla 3-1. Lista parcial de la configuración avanzada del sistema de seguridad (continuación)

Configuración avanzada del sistema	Descripción	Valor predeterminado
UserVars.DcuiTimeOut	Establece el tiempo de inactividad en los segundos antes de que el sistema cierre automáticamente la sesión de la DCUI. El valor 0 (cero) desactiva el tiempo de espera.	600 (10 minutos)
UserVars.ESXiShellInteractiveTimeOut	Establece el tiempo de inactividad en los segundos antes de que el sistema cierre automáticamente la sesión en un shell interactivo. Esta opción solo se aplica a las nuevas sesiones. El valor 0 (cero) desactiva el tiempo de inactividad. Se aplica tanto al shell SSH como a la DCUI.	0
UserVars.ESXiShellTimeOut	Establece el tiempo en los segundos que un shell de inicio de sesión espera para iniciar sesión. El valor 0 (cero) desactiva el tiempo de espera. Se aplica tanto al shell SSH como a la DCUI.	0
UserVars.HostClientSessionTimeout	Establece el tiempo de inactividad en los segundos antes de que el sistema cierre automáticamente la sesión de Host Client. El valor 0 (cero) desactiva el tiempo de inactividad.	900 (15 minutos)
UserVars.HostClientClientClientcomeMessage	Muestra un mensaje de bienvenida en Host Client al iniciar sesión. El mensaje se muestra después del inicio de sesión como una "sugerencia".	(Vacío)

Configurar hosts ESXi con Host Profiles

Los perfiles de host permiten establecer configuraciones estándar para los hosts ESXi y automatizar el cumplimiento de estas opciones de configuración. Los perfiles de host permiten controlar varios aspectos de la configuración de hosts, como la memoria, el almacenamiento, las redes, etc.

Los perfiles de host proporcionan un mecanismo administrado de forma central y automatizado para la configuración de hosts y el cumplimiento de la configuración. Los perfiles de host pueden mejorar la eficacia al reducir la dependencia de tareas manuales y repetitivas. Los perfiles de host capturan la configuración de un host de referencia preconfigurado y validado, almacenan la configuración como objeto administrado y utilizan el catálogo de los parámetros comprendidos para configurar la red, el almacenamiento, la seguridad y otros parámetros de nivel de host.

Se pueden configurar perfiles de host para un host de referencia desde vSphere Client y aplicar el perfil de host a todos los hosts que comparten las características del host de referencia. También se pueden usar perfiles de host para detectar cambios de configuración en los hosts. Consulte la documentación de *Perfiles de host de vSphere*.

Es posible asociar el perfil de host a un clúster para aplicarlo a todos los hosts de este.

Procedimiento

1 Configure el host de referencia de acuerdo con las especificaciones y cree un perfil de host.

2 Asocie el perfil a un host o un clúster.

3 Aplique el perfil de host del host de referencia a otros hosts o clústeres.

Usar scripts para administrar opciones de configuración de hosts ESXi

En los entornos con muchos hosts ESXi, la administración de hosts con scripts resulta más rápida y es menos proclive a errores que la administración de hosts desde vSphere Client.

vSphere incluye lenguajes de scripting para la administración de hosts ESXi. VMware PowerCLI es una interfaz de Windows PowerShell para vSphere API, e incluye cmdlets de PowerShell para administrar los componentes de vSphere. ESXCLI incluye un conjunto de comandos para administrar hosts ESXi y máquinas virtuales. Consulte https://developer.vmware.com para obtener información de referencia y sugerencias de programación. La documentación sobre el administrador de vSphere se centra en el uso de vSphere Client para la administración.

También se puede usar una de las interfaces de scripting en vSphere Automation SDK, como vSphere Automation SDK for Python.

Procedimiento

1 Cree una función personalizada con privilegios limitados.

   Consulte Crear una función personalizada de vCenter Server.

   Por ejemplo, considere crear una función que contenga un conjunto de privilegios para administrar hosts, pero que no incluya privilegios para administrar máquinas virtuales, almacenamiento o redes. Si el script que desea usar solamente extrae información, puede crear una función con privilegios de solo lectura para el host.

2 En vSphere Client, cree una cuenta de servicio y asigne la función personalizada a esa cuenta.

   Puede crear varias funciones personalizadas con diferentes niveles de acceso si desea que el acceso a determinados hosts sea bastante limitado.

3 Escriba scripts para comprobar o modificar parámetros, y ejecute esos scripts.

   Por ejemplo, puede comprobar o establecer el tiempo de espera interactivo del shell de un host de la siguiente manera:

Lenguaje	Comandos
ESXCLI	`esxcli <conn_options> system settings advanced get /UserVars/ESXiShellTimeOut` `esxcli --formatter=csv --format-param=fields="Path,Int Value" system settings advanced list | grep /UserVars/ESXiShellTimeOut`
PowerCLI	`#List UserVars.ESXiShellInteractiveTimeOut for each host Get-VMHost | Select Name, @{N="UserVars.ESXiShellInteractiveTimeOut";E={$_ | Get-AdvancedSetting -Name UserVars.ESXiShellInteractiveTimeOut | Select -ExpandProperty Value}}` `# Set UserVars.ESXiShellTimeOut to 900 on all hosts Get-VMHost | Foreach { Get-AdvancedSetting -Entity $_ -Name UserVars.ESXiShellInteractiveTimeOut | Set-AdvancedSetting -Value 900 }`

4 En entornos grandes, cree funciones con diferentes privilegios de acceso y hosts de grupos en carpetas según las tareas que desee realizar. Posteriormente, puede ejecutar scripts en diferentes carpetas desde diferentes cuentas de servicio.

5 Verifique que se hayan producido cambios después de ejecutar el comando.

Bloqueo de cuenta y contraseñas ESXi

Para los hosts ESXi, debe utilizar una contraseña con requisitos predefinidos. Puede cambiar el requisito de longitud requerida y la clase de caracteres o permitir frases de contraseña si utiliza el ajuste del sistema avanzado `Security.PasswordQualityControl`. También puede establecer el número de contraseñas para recordar para cada usuario mediante el ajuste del sistema avanzado `Security.PasswordHistory`.

Nota Los requisitos predeterminados para las contraseñas de ESXi pueden cambiar de una versión a otra. Puede comprobar las restricciones predeterminadas para la contraseña y modificarlas con el ajuste del sistema avanzado `Security.PasswordQualityControl`.

Contraseñas de ESXi

ESXi aplica requisitos de contraseña para el acceso desde la interfaz de usuario de la consola directa, ESXi Shell, SSH o VMware Host Client.

- De manera predeterminada, debe incluir una combinación de al menos tres de las cuatro clases de caracteres siguientes: letras en minúscula, letras en mayúscula, números y caracteres especiales, como el guion bajo o el guion, al crear una contraseña.
- De forma predeterminada, la longitud de la contraseña debe tener como mínimo 7 caracteres y menos de 40.
- Las contraseñas no deben contener una palabra de diccionario ni parte de una palabra de diccionario.
- Las contraseñas no deben contener el nombre de usuario ni partes del mismo.

Nota Un carácter en mayúscula al inicio de una contraseña no se tiene en cuenta en la cantidad de clases de caracteres que se utilizan. Un número al final de una contraseña no se tiene en cuenta en la cantidad de clases de caracteres que se utilizan. Una palabra del diccionario que se utiliza dentro de una contraseña reduce la longitud general de la contraseña.

Ejemplos de contraseñas de ESXi

A continuación se indican posibles contraseñas en caso de configurar la opción de la siguiente manera.

```
retry=3 min=disabled,disabled,disabled,7,7
```

Con esta opción, se solicita al usuario hasta tres veces (retry=3) una contraseña nueva si no es lo suficientemente segura o si la contraseña no se introdujo correctamente dos veces. No se permiten las contraseñas que tienen una o dos clases de caracteres ni las frases de contraseña, ya que los primeros tres elementos están desactivados. Las contraseñas de tres y cuatro clases de caracteres requieren siete caracteres. Consulte la página del manual de `pam_passwdqc` para obtener más información sobre otras opciones, como `max` y `passphrase`, entre otras.

Con esta configuración, se permiten las siguientes contraseñas.

- xQaTEhb!: contiene ocho caracteres de tres clases.
- xQaT3#A: contiene siete caracteres de cuatro clases.

Las siguientes contraseñas posibles no cumplen con los requisitos.

- Xqat3hi: comienza con un carácter en mayúscula, lo que reduce la cantidad efectiva de clases de caracteres a dos. La cantidad mínima de clases de caracteres requerida es tres.
- xQaTEh2: termina con un número, lo que reduce la cantidad efectiva de clases de caracteres a dos. La cantidad mínima de clases de caracteres requerida es tres.

Frase de contraseña de ESXi

En lugar de una contraseña, también puede utilizar una frase de contraseña. Sin embargo, las frases de contraseña están desactivadas de forma predeterminada. Puede cambiar este valor predeterminado u otros valores de configuración mediante el ajuste del sistema avanzado `Security.PasswordQualityControl` de vSphere Client.

Por ejemplo, puede cambiar la opción por la siguiente.

```
retry=3 min=disabled,disabled,16,7,7
```

Este ejemplo permite frases de contraseña de al menos 16 caracteres y al menos tres palabras.

Modificar las restricciones predeterminadas de contraseña

Puede cambiar la restricción predeterminada de contraseñas y frases de contraseña con el ajuste del sistema avanzado `Security.PasswordQualityControl` para su host ESXi. Consulte la documentación de *Administrar vCenter Server y hosts* para obtener información sobre cómo cambiar los ajustes avanzados del sistema de ESXi.

Puede cambiar el valor predeterminado, por ejemplo, para requerir un mínimo de 15 caracteres y una cantidad mínima de cuatro palabras (`passphrase=4`) de la siguiente manera:

```
retry=3 min=disabled,disabled,15,7,7 passphrase=4
```

Para obtener más información, consulte la página del manual de `pam_passwdqc`.

Nota Aún no se han probado todas las combinaciones posibles de opciones de contraseña. Después de cambiar la configuración de contraseña predeterminada, realice una prueba adicional.

En este ejemplo, se establece el requisito de complejidad de contraseña para requerir ocho caracteres de cuatro clases que aplican una diferencia significativa de contraseñas, un historial recordado de cinco contraseñas y una directiva de rotación de 90 días:

```
min=disabled,disabled,disabled,disabled,8 similar=deny
```

Comportamiento del bloqueo de cuentas de ESXi

Se admite el bloqueo de cuentas para el acceso a través de SSH y vSphere Web Services SDK. La interfaz de la consola directa (DCUI) y ESXi Shell no admiten el bloqueo de cuentas. De forma predeterminada, se permite un máximo de cinco intentos con errores antes de que la cuenta se bloquee. De forma predeterminada, la cuenta se desbloquea después de 15 minutos.

Configurar el comportamiento de inicio de sesión

Puede configurar el comportamiento de inicio de sesión del host ESXi con los siguientes ajustes del sistema avanzados:

- `Security.AccountLockFailures`. Cantidad máxima de intentos de inicio de sesión con errores antes de que la cuenta de un usuario se bloquee. Cero desactiva el bloqueo de cuentas.

- `Security.AccountUnlockTime`. Cantidad de segundos en los que el usuario queda bloqueado.
- `Security.PasswordHistory`. Número de contraseñas que se deben recordar para cada usuario. A partir de vSphere 8.0 Update 1, el valor predeterminado es cinco. Cero desactiva el historial de contraseñas.

Consulte la documentación de *Administrar vCenter Server y hosts* para obtener información sobre la configuración de las opciones avanzadas de ESXi.

Generación de claves criptográficas de ESXi

ESXi genera varias claves asimétricas para el funcionamiento normal. La clave de seguridad de la capa de transporte (Transport Layer Security, TLS) protege la comunicación con el host ESXi mediante el protocolo TLS. La clave SSH protege la comunicación con el host ESXi mediante el protocolo SSH.

Clave de seguridad de la capa de transporte

La clave de seguridad de la capa de transporte (TLS) protege la comunicación con el host mediante el protocolo TLS. Tras el primer arranque, el host ESXi genera la clave TLS como una clave RSA de 2048 bits. Actualmente, ESXi no implementa la generación automática de claves ECDSA para TLS. La clave privada de TLS no está pensada para que el administrador la procese.

La clave TLS reside en la siguiente ubicación no persistente:

```
/etc/vmware/ssl/rui.key
```

La clave pública TLS (incluidas las entidades de certificación intermedias) reside en la siguiente ubicación no persistente como un certificado X.509 v3:

```
/etc/vmware/ssl/rui.crt
```

Cuando se utiliza vCenter Server con los hosts ESXi, vCenter Server genera una CSR automáticamente, la firma mediante la entidad de certificación de VMware (VMware Certificate Authority, VMCA) y genera el certificado. Cuando se agrega un host ESXi a vCenter Server, vCenter Server instala el certificado resultante en el host ESXi.

El certificado TLS predeterminado se autofirma, con un campo subjectAltName que coincide con el nombre de host durante la instalación. Puede instalar un certificado diferente, por ejemplo, para utilizar un subjectAltName diferente o para incluir una entidad de certificación (Certificate Authority, CA) en particular en la cadena de verificación. Consulte Reemplazar el certificado de ESXi predeterminado por un certificado personalizado.

Clave SSH

La clave SSH protege la comunicación con el host ESXi mediante el protocolo SSH. Tras el primer arranque, el sistema genera una clave ECDSA nistp256 y las claves SSH como claves RSA de 2048 bits. El servidor SSH está desactivado de forma predeterminada. El acceso SSH está destinado principalmente a fines de solución de problemas. Las claves SSH no están pensadas para que el administrador las procese. El inicio de sesión a través de SSH requiere privilegios administrativos equivalentes al control total del host. Para habilitar el acceso SSH, consulte Activar el acceso a ESXi Shell mediante vSphere Client.

Las claves públicas SSH residen en la siguiente ubicación:

`/etc/ssh/ssh_host_rsa_key.pub`

`/etc/ssh/ssh_host_ecdsa_key.pub`

Las claves privadas SSH residen en la siguiente ubicación:

`/etc/ssh/ssh_host_rsa_key`

`/etc/ssh/ssh_host_ecdsa_key`

Establecimiento de clave criptográfica TLS

La configuración del establecimiento de claves criptográficas TLS se rige por la elección de conjuntos de claves de cifrado TLS, que seleccionan acuerdos de claves basados en ECC mediante el uso de acuerdos de clave de Ecliptic Curve Diffie Hellman (ECDH) efímeros (como se especifica en la publicación especial 800-56A de NIST).

Establecimiento de clave criptográfica SSH

La configuración del establecimiento de la clave criptográfica SSH se rige por la configuración de SSHD. ESXi proporciona una configuración predeterminada que permite el acuerdo de clave Diffie-Hellman (DH) efímero (según se especifica en la publicación especial NIST 800-56A) y el acuerdo de clave Ecliptic Curve Diffie Hellman (ECHD) efímero (como se especifica en la publicación especial 800-56A de NIST). La configuración de SSHD no está pensada para que el administrador la procese.

Seguridad de SSH en ESXi

La interfaz de ESXi Shell y la interfaz SSH están desactivadas de forma predeterminada. Mantenga estas interfaces desactivadas a menos que esté realizando actividades de solución de problemas o de soporte. Para las actividades cotidianas, utilice vSphere Client, donde la actividad está sujeta al control de acceso basado en funciones y a métodos de control de acceso modernos.

Configuración de SSH en ESXi

La configuración de SSH en ESXi utiliza las siguientes opciones.

Protocolo SSH versión 1 desactivado

VMware no admite el protocolo SSH versión 1 y usa el protocolo versión 2 de forma exclusiva. La versión 2 elimina determinados problemas de seguridad que tiene la versión 1 y ofrece una forma segura de comunicarse con la interfaz de administración.

Intensidad de cifrado mejorada

SSH admite solo cifrados AES de 256 y 128 bits para las conexiones.

Está configuración está diseñada para proporcionar una protección sólida de los datos que se transmiten a la interfaz de administración a través de SSH. Esta configuración no se puede cambiar.

Claves SSH de ESXi

Las claves SSH pueden restringir, controlar y proteger el acceso a un host ESXi. Una clave SSH puede permitir que un usuario de confianza o un script inicien sesión en un host sin especificar una contraseña.

También puede utilizar el método PUT de HTTPS para copiar la clave SSH en el host.

En lugar de generar claves de forma externa y cargarlas, es posible crearlas en el host ESXi y descargarlas. Consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/1002866.

Habilitar SSH y agregar claves SSH al host presenta riesgos innatos. Compare el riesgo potencial de exponer un nombre de usuario y una contraseña contra el riesgo de intromisión de un usuario que tenga una clave confiable.

Cargar una clave SSH mediante el método PUT de HTTPS

Puede utilizar claves autorizadas para iniciar sesión en un host con SSH. Puede cargar las claves autorizadas mediante el método PUT de HTTPS.

Las claves autorizadas permiten autenticar el acceso remoto a un host. Cuando los usuarios o scripts intentan acceder a un host con SSH, la clave proporciona la autenticación sin solicitar una contraseña. Las claves autorizadas permiten automatizar la autenticación, lo cual resulta útil para escribir scripts que realizan tareas de rutina.

Puede cargar en un host los siguientes tipos de claves SSH mediante el método PUT de HTTPS:

- Archivo de claves autorizadas para el usuario raíz
- Clave DSA
- Clave pública de DSA
- Clave de RSA
- Clave pública de RSA

Importante No modifique el archivo `/etc/ssh/sshd_config`.

Procedimiento

1 En la aplicación de carga, abra el archivo de claves.

2 Publique el archivo en las siguientes ubicaciones.

Tipo de clave	Ubicación
Archivos de claves autorizadas para el usuario raíz	`https://`*`hostname_or_IP_address`*`/host/ssh_root_authorized_keys` Debe tener privilegios completos de administrador sobre el host para poder cargar el archivo.
Claves DSA	`https://`*`hostname_or_IP_address`*`/host/ssh_host_dsa_key`
Claves públicas DSA	`https://`*`hostname_or_IP_address`*`/host/ssh_host_dsa_key_pub`
Claves RSA	`https://`*`hostname_or_IP_address`*`/host/ssh_host_rsa_key`
Claves públicas RSA	`https://`*`hostname_or_IP_address`*`/host/ssh_host_rsa_key_pub`

Dispositivos PCI/PCIe y ESXi

El uso de VMware DirectPath I/O para establecer el acceso directo de un dispositivo PCI o PCIe a una máquina virtual representa una vulnerabilidad potencial de la seguridad. La vulnerabilidad se puede activar debido a que un código malintencionado o defectuoso (como un controlador de dispositivo) se ejecuta en modo privilegiado en el sistema operativo invitado. Actualmente, el hardware y el firmware estándar del sector no admiten la contención de errores para proteger los hosts ESXi de esta vulnerabilidad.

Use el acceso directo PCI o PCIe a una máquina virtual solo si una entidad de confianza posee y administra la máquina virtual. Es necesario tener la certeza de que esta entidad no intentará bloquear o aprovechar el host de la máquina virtual.

Es posible que el host quede comprometido de una de las siguientes maneras.

- El sistema operativo invitado puede generar un error de PCI o PCIe irrecuperable. Un error de ese tipo no daña los datos, pero puede bloquear el host ESXi. Esos errores pueden ser resultado de errores o incompatibilidades en los dispositivos de hardware para los que se establecen accesos directos. Otros motivos para los errores incluyen problemas con los controladores en el sistema operativo invitado.
- El sistema operativo invitado puede generar una operación de acceso directo a memoria (DMA) que provoque un error de página IOMMU en el host ESXi. Esta operación podría ser el resultado de una operación de DMA cuyo objetivo fuera una dirección fuera de la memoria de la máquina virtual. En algunas máquinas, el firmware del host configura los errores de IOMMU para que notifiquen un error irrecuperable a través de una interrupción no enmascarable (NMI). Este error irrecuperable hace que el host ESXi se bloquee. La causa de esto pueden ser problemas con los controladores en el sistema operativo invitado.
- Si el sistema operativo en el host ESXi no utiliza la reasignación de interrupciones, es posible que el sistema operativo invitado inyecte una interrupción falsa en el host ESXi en cualquier vector. Actualmente, ESXi utiliza la reasignación de interrupciones en las plataformas Intel

donde se encuentra disponible. La asignación de interrupciones forma parte del conjunto de características de Intel VT-d. ESXi no utiliza la asignación de interrupciones en las plataformas AMD. Una interrupción falsa puede bloquear el host ESXi. En teoría, es posible que existan otras formas de aprovechar estas interrupciones falsas.

Desactivar el explorador de objetos administrados de vSphere

El explorador de objetos administrados (Managed Object Browser, MOB) es una utilidad de vSphere que permite explorar el modelo de objetos VMkernel. Sin embargo, los atacantes pueden utilizar esta interfaz para realizar acciones o cambios maliciosos en la configuración porque se puede cambiar la configuración del host desde el MOB. Utilice el MOB únicamente para depurar y asegúrese de que esté desactivado en los sistemas de producción.

El MOB está desactivado de forma predeterminada. Sin embargo, es necesario utilizar el MOB para ciertas tareas, por ejemplo, para extraer un certificado antiguo de un sistema. Puede activar o desactivar el MOB de la siguiente manera.

Procedimiento

1 Desplácese hasta el host en el inventario de vSphere Client.

2 Haga clic en **Configurar**.

3 En Sistema, haga clic en **Configuración avanzada del sistema**.

4 Compruebe el valor de **Config.HostAgent.plugins.solo.enableMob** y haga clic en **Editar** para cambiarlo según corresponda.

   No utilice `vim-cmd` desde ESXi Shell.

Recomendaciones de seguridad para redes de ESXi

El aislamiento del tráfico de red es fundamental para proteger el entorno de ESXi. Las distintas redes requieren diferente acceso y nivel de aislamiento.

El host ESXi usa varias redes. Emplee las medidas de seguridad que correspondan para cada red y aísle el tráfico de aplicaciones y funciones específicas. Por ejemplo, asegúrese de que el tráfico de VMware vSphere® vMotion® no pase por redes en las que haya máquinas virtuales. El aislamiento impide las intromisiones. Además, por motivos de rendimiento, también se recomienda usar redes separadas.

- Las redes de infraestructura de vSphere se usan para funciones como vSphere vMotion, VMware vSphere Fault Tolerance, VMware vSAN y almacenamiento. Aísle estas redes según sus funciones específicas. Generalmente, no es necesario dirigir estas redes fuera de un rack de servidor físico único.
- Una red de administración aísla los distintos tráficos (tráfico de clientes, de la interfaz de la línea de comandos (CLI) o de la API, y del software de terceros) de otros tráficos. En general, solo los administradores de sistemas, redes y seguridad pueden acceder a la red de administración. Para proteger el acceso a la red de administración, utilice un host bastión o una red privada virtual (VPN). Controle estrictamente el acceso dentro de esta red.

- El tráfico de las máquinas virtuales puede transmitirse por medio de una red o de muchas. Puede optimizar el aislamiento de las máquinas virtuales mediante soluciones de firewall virtuales que establezcan reglas de firewall en la controladora de red virtual. Esta configuración se envía junto con una máquina virtual cuando esta se migra de un host a otro dentro del entorno de vSphere.

Modificar la configuración del proxy web de ESXi

Al modificar la configuración del proxy web, hay varias directrices de seguridad del usuario y del cifrado que se deben tener en cuenta.

Nota Reinicie el proceso del host después de realizar cualquier cambio en los directorios o los mecanismos de autenticación del host.

- No configure certificados que utilicen una contraseña o frases de contraseña. ESXi no es compatible con proxies web que utilizan contraseñas o frases de contraseña, llamadas también claves cifradas. Si se configura un proxy web que requiere una contraseña o una frase de contraseña, los procesos de ESXi no podrán iniciarse correctamente.
- Para que resulte compatible el cifrado de los nombres de usuario, las contraseñas y los paquetes, SSL se activa de forma predeterminada en las conexiones de vSphere Web Services SDK. Si desea configurar estas conexiones de modo que no cifren las transmisiones, desactive SSL en la conexión de vSphere Web Services SDK. Para ello, cambie la conexión de HTTPS a HTTP.

  Considere desactivar SSL solo si creó un entorno de plena confianza para estos clientes, donde los firewalls estén establecidos y las transmisiones desde y hacia el host estén aisladas por completo. Si se desactiva SSL, se puede mejorar el rendimiento debido a que se evita la sobrecarga requerida para el cifrado.
- Para evitar la utilización incorrecta de los servicios de ESXi, se puede acceder a la mayoría de los servicios internos de ESXi únicamente mediante el puerto 443, el puerto utilizado para la transmisión de HTTPS. El puerto 443 funciona como un proxy inverso de ESXi. Se puede ver la lista de servicios en ESXi a través de la página principal de HTTP, pero no se puede acceder directamente a los servicios de adaptadores de almacenamiento sin la debida autorización.

  Se puede cambiar esta configuración de modo que los servicios individuales sean accesibles directamente a través de las conexiones de HTTP. No realice este cambio, a menos que utilice ESXi en un entorno de plena confianza.
- Al actualizar el entorno, el certificado permanece en su ubicación.

Consideraciones de seguridad de vSphere Auto Deploy

Cuando utilice vSphere Auto Deploy, preste especial atención a la seguridad de redes, a la seguridad de la imagen de arranque y a la posible exposición de la contraseña en los perfiles de host para proteger su entorno.

Seguridad de redes

Asegure su red igual que si se tratara de cualquier otro método de implementación basado en PXE. vSphere Auto Deploy transfiere datos por SSL para evitar interferencias accidentales e intromisiones. Sin embargo, la autenticidad del cliente o del servidor Auto Deploy no se comprueba durante un arranque PXE.

Puede reducir ampliamente el riesgo de seguridad de Auto Deploy aislando por completo la red donde se utiliza Auto Deploy.

Imagen de arranque y seguridad de perfil de host

La imagen de arranque que descarga el servidor vSphere Auto Deploy en una máquina puede tener los siguientes componentes.

- Los paquetes de VIB que componen el perfil de imagen se incluyen siempre en la imagen de arranque.
- El perfil de host y la personalización del host se incluyen en la imagen de arranque si las reglas de Auto Deploy se configuran para aprovisionar el host con un perfil o una personalización del host.
  - La contraseña de administrador (raíz) y las contraseñas de usuario que se incluyen en el perfil de host y en la personalización de host están cifradas con hash SHA-512.
  - Cualquier otra contraseña asociada a los perfiles quedará excluida. Si configura Active Directory utilizando perfiles de host, las contraseñas no poseen protección.

    Utilice vSphere Authentication Proxy para evitar la exposición de las contraseñas de Active Directory. Si configura Active Directory utilizando perfiles de host, las contraseñas no están protegidas.
- El certificado y la clave SSL públicas y privadas del host se incluyen en la imagen de arranque.

Acceso de control para herramientas de supervisión de hardware basadas en CIM

El sistema del modelo de información común (CIM) proporciona una interfaz para que aplicaciones remotas supervisen los recursos de hardware mediante un conjunto de interfaces de programación de aplicaciones (API) estándar. Para garantizar que la interfaz de CIM sea segura, proporcione únicamente el acceso mínimo y necesario a estas aplicaciones remotas. Si aprovisiona una aplicación remota con una cuenta raíz o de administrador y si la aplicación está comprometida, puede comprometerse el entorno virtual.

CIM es un estándar abierto que establece un marco para la supervisión de recursos de hardware sin agente basada en estándares para hosts ESXi. Este marco consta de un administrador de objetos CIM, a menudo llamado agente CIM, y un conjunto de proveedores CIM.

Los proveedores de CIM admiten acceso de administración para controladores de dispositivos y hardware subyacente. Los proveedores de hardware, incluidos los fabricantes de servidores y los proveedores de dispositivos de hardware, pueden escribir proveedores que supervisen y administren sus dispositivos. VMware escribe proveedores que supervisan hardware de servidor, infraestructura de almacenamiento de ESXi y recursos específicos de virtualización. Estos proveedores se ejecutan dentro del host ESXi. Son livianos y se centran en tareas específicas de administración. El agente CIM toma información de todos los proveedores de CIM y usa API estándar para presentar la información al mundo exterior. La API más común es WS-MAN.

No proporcione credenciales de raíz a aplicaciones remotas que accedan a la interfaz de CIM. En su lugar, cree una cuenta de usuario de vSphere con menos privilegios para estas aplicaciones y utilice la función de ticket de API de VIM para emitir un valor de sessionId (denominado "ticket") para esta cuenta de usuario con menos privilegios para autenticarse en CIM. Si se le concede un permiso a la cuenta para obtener tickets de CIM, la API de VIM puede proporcionar el ticket a CIM. A continuación, estos tickets se proporcionan como la contraseña y el identificador de usuario a cualquier llamada API de CIM-XML. Consulte el método `AcquireCimServicesTicket()` para obtener más información.

El servicio CIM se inicia cuando se instala un CIM VIB de terceros (por ejemplo, cuando se ejecuta el comando `esxcli software vib install -n` *`VIBname`*).

Si debe activar el servicio CIM manualmente, ejecute el siguiente comando:

```
esxcli system wbem set -e true
```

Si es necesario, puede desactivar wsman (servicio WSManagement) para que se ejecute solamente el servicio CIM:

```
esxcli system wbem set -W false
```

Para confirmar que wsman está desactivado, ejecute el siguiente comando:

```
esxcli system wbem get
…
WSManagement PID: 0
WSManagement Service: false
```

Para obtener más información sobre los comandos ESXCLI, consulte la *documentación de ESXCLI*. Para obtener más información sobre cómo activar el servicio CIM, consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/1025757.

Procedimiento

1 Cree una cuenta de usuario no raíz de vSphere para las aplicaciones de CIM.

   Consulte el tema sobre cómo agregar usuarios de vCenter Single Sign-On en *vSphere Authentication*. El privilegio de vSphere necesario para la cuenta de usuario es **Host.CIM.Interacción**.

2 Utilice el SDK de vSphere API que desee para autenticar la cuenta de usuario en vCenter Server. A continuación, realice una llamada a `AcquireCimServicesTicket()` para devolver un ticket con el fin de autenticarse con ESXi como una cuenta de nivel de administrador mediante las API del puerto 5989 de CIM-XML o del puerto 433 de WS-Man.

   Consulte *Referencia de vSphere Web Services API* para obtener más información.

3 Renueve el ticket cada dos minutos según sea necesario.

Prácticas recomendadas de seguridad de vSphere Distributed Services Engine

Para maximizar la seguridad de su entorno de ESXi, siga las prácticas recomendadas para vSphere Distributed Services Engine.

En vSphere 8.0 y versiones posteriores, vSphere Distributed Services Engine permite la descarga de funciones de infraestructura desde las CPU de un host o un servidor en unidades de procesamiento de datos (Data Processing Units, DPU), también conocidas como "SmartNIC", lo que libera ciclos de CPU para atender a las aplicaciones. Para obtener una introducción a vSphere Distributed Services Engine, consulte la documentación de *Instalar y configurar VMware ESXi*. Para obtener más información sobre vSphere Distributed Services Engine, consulte la documentación de *Administración del ciclo de vida de hosts y clústeres*.

En general, trate los aspectos de seguridad de vSphere Distributed Services Engine como hace al proteger el entorno de ESXi.

- La interfaz de ESXi Shell y la interfaz SSH para vSphere Distributed Services Engine están desactivadas de forma predeterminada. Mantenga estas interfaces desactivadas a menos que esté realizando actividades de solución de problemas o de soporte.
- Para las actividades de administración cotidianas de vSphere Distributed Services Engine, utilice vSphere Client, donde la actividad está sujeta al control de acceso basado en funciones y a métodos de control de acceso modernos.

Controlar la entropía de ESXi

En ESXi 8.0 y versiones posteriores, la implementación de entropía de ESXi admite las certificaciones FIPS 140-3 y EAL4. Las opciones de arranque del kernel controlan qué orígenes de entropía se activan en un host ESXi.

En computación, el término "entropía" hace referencia a los caracteres aleatorios y los datos que se recopilan para su uso en criptografía, como la generación de claves de cifrado para proteger los datos transmitidos a través de una red. La seguridad requiere entropía para generar claves y comunicarse de forma segura a través de la red. La entropía a menudo se recopila entre una variedad de orígenes en un sistema.

El manejo de entropía de FIPS es el comportamiento predeterminado si se cumplen las siguientes condiciones.

1 El hardware es compatible con RDSEED.

2 La opción de arranque de VMkernel disableHwrng no está presente o es FALSE.

3 La opción de arranque de VMkernel entropySources no está presente, es 0 (cero) o es 4.

Advertencia Cuando configura un host ESXi con entropySources solo para entropía externa (es decir, entropySources se establece en 8), debes seguir suministrando la entropía externa al host utilizando la API de entropía. Si se agota la entropía en el host, este deja de responder. Para recuperarse de esta situación, reinicie el host. Si el host sigue sin responder, debe volver a instalar ESXi.

A partir de ESXi 8.0 Update 1, es posible configurar orígenes de entropía externos en el archivo de inicio de una instalación generada por script. Puede configurar ESXi en un entorno de alta seguridad para consumir entropía de orígenes de entropía externos, como un módulo de seguridad de hardware (Hardware Security Module, HSM), y alinearse con estándares como BSI Common Criteria, EAL4 y NIST FIPS CMVP, mediante el método de instalación por script. Para obtener más información sobre la configuración de fuentes de entropía externas, consulte la documentación de *Instalar y configurar VMware ESXi*.

Puede configurar el subsistema de entropía de ESXi mediante las siguientes opciones de arranque de VMkernel:

Tabla 3-2. Opciones de arranque de VMkernel de entropía de ESXi

Opción de arranque de VMkernel	Tipo de opción	Descripción	Valor predeterminado
disableHwrng (disponible antes de vSphere 8.0)	Booleano	Desactiva los orígenes de entropía RDRAND y RDSEED cuando se establecen en TRUE (reemplaza a "entropySources").	FALSE Si está presente, activa orígenes de entropía del generador de números aleatorios del hardware.
entropySources (disponible a partir de vSphere 8.0)	Entero, máscara de bits	Especifica qué orígenes de entropía se activarán. ■ 0 (predeterminado) Valores de máscara de bits: ■ 1 = interrupciones ■ 2 = RDRAND ■ 4 = RDSEED ■ 8 = entropyd (la gestión de entropía de EAL4 está activada) Al especificar entropySources = 9, se activan las interrupciones y los orígenes de entropía del espacio de usuario, y se desactivan los orígenes de entropía RDRAND y RDSEED.	0 (cero) Si se admite RDSEED, el valor predeterminado es la conformidad con FIPS. De lo contrario, el valor predeterminado son todos los orígenes de entropía, excepto entropyd.

Nota Antes de hacer un cambio para usar únicamente los orígenes de entropía RDRAND, RDSEED o ambos, compruebe la documentación del proveedor para asegurarse de que el host ESXi admita dichas configuraciones. Si el host no admite esas configuraciones, vCenter Server le enviará una alerta y el host volverá a usar los orígenes de entropía de espacio de usuario e interrupciones.

Requisitos previos

Debe tener acceso raíz en el host ESXi.

Procedimiento

1 Utilice SSH u otra conexión de consola remota para iniciar una sesión en el host de ESXi.

2 Inicie sesión como raíz.

3 Establezca las opciones de arranque de VMkernel de entropía que desee.

a Para desactivar los orígenes de entropía RDRAND y RDSEED para disableHwrng:

```
esxcli system settings kernel set -s disableHwrng -v TRUE
```

b Para establecer entropySources:

```
esxcli system settings kernel set -s entropySources -v entropy_source_value
```

Consulte la tabla anterior para ver los valores que se pueden establecer para entropySources.

Administrar certificados para hosts ESXi

La entidad de certificación de VMware (VMware Certificate Authority, VMCA) aprovisiona a cada host ESXi nuevo con un certificado firmado cuya entidad de certificación raíz predeterminada es VMCA. El aprovisionamiento se produce cuando se agrega un host a vCenter Server explícitamente, o bien como parte de la instalación o la actualización de ESXi.

Puede ver y administrar certificados de ESXi desde vSphere Client y con la API de `vim.CertificateManager` en vSphere Web Services SDK. No puede ver ni administrar los certificados de ESXi por medio de las CLI de administración de certificados que están disponibles para administrar certificados de vCenter Server.

A partir de vSphere 8.0 Update 3, puede reemplazar los certificados de ESXi sin poner el host en modo de mantenimiento y sin tener que reiniciar el host o los servicios individuales.

Certificados y modos de certificación

Cuando ESXi y vCenter Server se comunican, estas utilizan TLS para casi todo el tráfico de administración.

vCenter Server admite los siguientes certificados y modos de certificación para hosts ESXi.

Tabla 3-3. Modos de certificación para hosts ESXi

Modo de certificación	Descripción
VMware Certificate Authority (predeterminada)	De forma predeterminada, se usa VMware Certificate Authority como entidad de certificación para los certificados de hosts ESXi. VMCA es la entidad de certificación raíz predeterminada, pero se puede configurar como la entidad de certificación intermedia de otra entidad. En el modo **vmca**, es posible renovar y actualizar los certificados desde vSphere Client. También se usa si VMCA es un certificado subordinado.
Entidad de certificación personalizada	Utilice este modo si desea utilizar solamente certificados personalizados que estén firmados por una entidad de certificación externa o empresarial. En el modo **personalizado**, la administración de los certificados es responsabilidad suya. A partir de vSphere 8.0 Update 3, puede administrar certificados personalizados desde vSphere Client. **Nota** A menos que cambie el modo de certificación al modo Entidad de certificación personalizada (**personalizado**), VMCA podrá reemplazar los certificados personalizados, por ejemplo, al seleccionar **Renovar** en vSphere Client.
Modo de huella digital	vSphere 5.5 usaba el modo **huella digital**, el cual todavía está disponible como opción de reserva para vSphere 6.x. En este modo, vCenter Server verifica que el certificado tenga el formato correcto, pero no verifica la validez del certificado. Se aceptan incluso los certificados que caducaron. No utilice este modo a menos que detecte problemas con uno de los otros dos modos y no pueda solucionarlos. Algunos servicios de vCenter Server 6.x y de versiones posteriores podrían funcionar mal en el modo de huella digital.

Para cambiar el modo de certificación y utilizar un tipo de certificado diferente, consulte Flujos de trabajo de cambio de modo de certificado de ESXi y Cambiar el modo de certificado de ESXi.

Caducidad de los certificados de ESXi

Puede ver información sobre la caducidad de los certificados firmados por VMCA o por una entidad de certificación externa en vSphere Client. Puede ver la información de todos los hosts que vCenter Server administra o de hosts individuales. Una alarma de color amarillo se enciende si el certificado se encuentra en estado **Por caducar en breve** (dentro de menos de ocho meses). Una alarma de color rojo se enciende si el certificado se encuentra en estado **Caducidad inminente** (dentro de menos de dos meses).

Certificados y aprovisionamiento de ESXi

Cuando inicia un host ESXi desde los medios de instalación, el host en principio tiene un certificado autogenerado. Cuando se agrega un host al sistema vCenter Server, vCenter Server aprovisiona el host con un certificado firmado por VMCA como CA raíz.

También se pueden utilizar certificados personalizados firmados por un tercero o una entidad de certificación empresarial para hosts ESXi.

Certificados y aprovisionamiento de ESXi en Auto Deploy

El proceso es similar para los hosts aprovisionados con Auto Deploy. No obstante, dado que esos hosts no almacenan ningún estado, el servidor Auto Deploy almacena el certificado firmado en su almacén local de certificados. El certificado se vuelve a utilizar en los arranques subsiguientes de los hosts ESXi. Un servidor Auto Deploy forma parte de cualquier implementación integrada o sistema de vCenter Server.

Si VMCA no está disponible cuando un host Auto Deploy se inicia por primera vez, el host primero intenta conectarse. Si el host no puede conectarse, realiza un ciclo de apagado y reinicio hasta que VMCA está disponible y el host puede aprovisionarse con un certificado firmado.

Puede hacer que Auto Deploy sea una entidad de certificación subordinada de una entidad de certificación de terceros. En este caso, los certificados generados se firman con la clave SSL de Auto Deploy. Consulte Convertir a Auto Deploy en una autoridad de certificación subordinada.

En ESXi 8.0 y versiones posteriores, puede utilizar certificados personalizados (firmados por una entidad de certificación) con Auto Deploy. Cuando se inicia el host, Auto Deploy asocia el certificado personalizado con una dirección MAC o el UUID del BIOS del host ESXi. Consulte Usar certificados personalizados con Auto Deploy.

Privilegios necesarios para la administración de certificados de ESXi

El privilegio de **Certificados.Administrar certificados** es necesario para que los usuarios administren los certificados del host ESXi.

Cambios en la dirección IP y el nombre de host ESXi

Un cambio en el nombre de host ESXi o la dirección IP podría afectar si vCenter Server considera que un certificado de host es válido o no. El modo en que se agregó el host ESXi a vCenter Server puede hacer que sea necesario una intervención manual. Por intervención manual se entiende que se debe volver a conectar el host, o bien se lo debe quitar de vCenter Server y volver a agregar.

Tabla 3-4. Cuando el nombre de host o la dirección IP se deben cambiar de forma manual

Se agregó un host ESXi a vCenter Server mediante...	Cambios en el nombre del host ESXi	Cambios en la dirección IP de ESXi
Nombre de host	Problema de conectividad de vCenter Server. Se necesita una intervención manual.	No se debe realizar ninguna acción.
Dirección IP	No se debe realizar ninguna acción.	Problema de conectividad de vCenter Server. Se necesita una intervención manual.

Certificados y actualizaciones de hosts ESXi

Si actualiza un host ESXi a ESXi 6.7 o una versión posterior, el proceso de actualización reemplaza los certificados autofirmados (huella digital) por certificados firmados por VMCA. Si el host ESXi utiliza certificados personalizados, el proceso de actualización conserva esos certificados aun si caducaron o no son válidos.

El flujo de trabajo recomendado para actualizar depende de los certificados actuales.

Host aprovisionado con certificados de huellas digitales

Si el host actualmente usa certificados de huellas digitales, se le asignan certificados de VMCA de manera automática como parte del proceso de actualización.

Nota No se pueden aprovisionar hosts heredados con certificados de VMCA. Debe actualizar estos hosts a ESXi 6.7 o una versión posterior.

Host aprovisionado con certificados personalizados

Si el host se aprovisiona con certificados personalizados (por lo general, certificados externos firmados por entidades de certificación), esos certificados permanecen en su lugar durante la actualización. Cambie el modo de certificado a **Personalizado** para asegurarse de no reemplazar accidentalmente los certificados durante una actualización de certificados posterior.

Nota Si el entorno se encuentra en modo VMCA y se actualizan los certificados desde vSphere Client, todos los certificados existentes se reemplazan por certificados firmados por VMCA.

Posteriormente, vCenter Server supervisa los certificados y muestra información, como la caducidad del certificado, en vSphere Client.

Hosts aprovisionados con Auto Deploy

Siempre se asignan nuevos certificados a los hosts que aprovisiona Auto Deploy cuando se arrancan por primera vez con el software ESXi 6.7 o una versión posterior. Al actualizar un host aprovisionado por Auto Deploy, el servidor Auto Deploy genera una solicitud de firma del certificado (CSR) para el host y la envía a VMCA. VMCA almacena el certificado firmado para el host. Cuando el servidor Auto Deploy aprovisiona el host, este recupera el certificado de VMCA y lo incluye en el proceso de aprovisionamiento.

Puede utilizar Auto Deploy con certificados personalizados.

Consulte Convertir a Auto Deploy en una autoridad de certificación subordinada y Usar certificados personalizados con Auto Deploy.

Flujos de trabajo de cambio de modo de certificado de ESXi

De forma predeterminada, VMware Certificate Authority (VMCA) aprovisiona a ESXi con certificados. Utilice el modo personalizado al reemplazar certificados de VMCA por certificados personalizados. Utilice el modo de huella digital heredado para la depuración. Si el cambio de modo es necesario, revise el posible impacto que puede provocar antes de realizarlo.

Para obtener una explicación sobre los modos de certificación, consulte Certificados y modos de certificación.

Usar certificados ESXi personalizados

Nota Al cambiar del uso de certificados de VMCA a certificados personalizados, asegúrese de dar tiempo a los procesos de aprobación y procesamiento de la organización cuando se generen los certificados. Además, planifique en consecuencia para que el certificado actual no caduque durante el cambio.

Si la directiva de la empresa exige que se use una entidad de certificación raíz distinta de VMCA, puede cambiar el modo de certificación en el entorno después de una minuciosa planificación. El siguiente es el flujo de trabajo.

1 Cambie al modo **personalizado**. Consulte Cambiar el modo de certificado de ESXi.

   Al cambiar el modo, vSphere Client activará el menú desplegable **Administrar con CA externa** para que pueda generar la solicitud de firma del certificado.

2 Agregue el certificado raíz de la entidad de certificación personalizada a VMware Endpoint Certificate Store (VECS).

3 Genere la solicitud de firma del certificado y obtenga los certificados que desea utilizar.

   Es posible que tenga que esperar un tiempo para que se devuelva la solicitud de firma del certificado.

4 Importe el certificado de CA personalizado en el host vCenter Server.

   Espere un tiempo a que vCenter Server distribuya el certificado de CA personalizado a los hosts ESXi.

Cambiar del modo de entidad de certificación personalizada al modo VMCA

Si está usando el modo de entidad de certificación personalizada y cree que el modo VMCA puede funcionar mejor en su entorno, puede realizar el cambio de modo después de una minuciosa planificación. El siguiente es el flujo de trabajo.

1 Quite todos los hosts del sistema vCenter Server.

2 En el sistema vCenter Server, elimine de VECS el certificado raíz de la entidad de certificación externa.

3 Cambie al modo **vmca**. Consulte Cambiar el modo de certificado de ESXi.

4 Agregue los hosts al sistema vCenter Server.

Nota Si sigue otro flujo de trabajo para este cambio de modo, se puede generar un comportamiento impredecible.

Conservar los certificados del modo de huella digital durante la actualización

El cambio del modo VMCA al modo de huella digital puede resultar necesario si se producen problemas con los certificados de VMCA. En el modo de huella digital, el sistema vCenter Server comprueba que exista un solo certificado y que su formato sea el correcto, pero no comprueba si el certificado es válido. Consulte Cambiar el modo de certificado de ESXi para obtener instrucciones.

Cambiar del modo de huella digital al modo VMCA

Si usa el modo de huella digital y desea comenzar a usar certificados firmados por VMCA, debe planificar un poco el cambio. El siguiente es el flujo de trabajo.

1 Quite todos los hosts ESXi del sistema vCenter Server.

2 Cambie al modo **vmca**. Consulte Cambiar el modo de certificado de ESXi.

3 Agregue los hosts ESXi al sistema vCenter Server.

Nota Si sigue otro flujo de trabajo para este cambio de modo, se puede generar un comportamiento impredecible.

Cambiar del modo de entidad de certificación personalizada al modo de huella digital

Si experimenta problemas con la entidad de certificación personalizada, considere cambiar temporalmente al modo de huella digital. El cambio se ejecutará sin problemas si sigue las instrucciones detalladas en Cambiar el modo de certificado de ESXi. Después de cambiar el modo, el sistema vCenter Server comprueba solamente el formato del certificado y ya no comprueba la validez del certificado.

Cambiar del modo de huella digital al modo de entidad de certificación personalizada

Si establece el entorno en el modo de huella digital durante la solución de problemas y desea comenzar a usar el modo de entidad de certificación personalizada, primero debe generar los certificados necesarios. El siguiente es el flujo de trabajo.

1 Quite todos los hosts ESXi del sistema vCenter Server.

2 Agregue el certificado raíz de la entidad de certificación personalizada al almacén TRUSTED_ROOTS de VECS en el sistema vCenter Server. Consulte Actualizar el almacén TRUSTED_ROOTS de vCenter Server (certificados personalizados).

3 En cada host ESXi:

   a Implemente la clave y el certificado de la entidad de certificación personalizada.

   b Reinicie los servicios del host.

4 Cambie al modo **personalizado**. Consulte Cambiar el modo de certificado de ESXi.

5 Agregue los hosts ESXi al sistema vCenter Server.

Configuración predeterminada de certificados ESXi

Cuando se agrega un host al sistema vCenter Server, vCenter Server envía una solicitud de firma de certificado (CSR) para el host en VMCA. Muchos de los valores predeterminados son adecuados para diversas situaciones, pero la información específica de la empresa puede cambiarse.

Puede cambiar varios de los valores predeterminados mediante vSphere Client. Considere cambiar la información de la organización y ubicación. Consulte Cambiar la configuración predeterminada de certificados de ESXi.

Tabla 3-5. Configuración de CSR ESXi

Parámetro	Valor predeterminado	Opción avanzada
Tamaño de clave	2048	N.A.
Algoritmo de clave	RSA	N.A.
Algoritmo de firma de certificado	sha256WithRSAEncryption	N.A.
Nombre común	Nombre del host si este se agregó a vCenter Server por nombre de host. Dirección IP del host si este se agregó a vCenter Server por dirección IP.	N.A.
País	EE. UU.	vpxd.certmgmt.certs.cn.country
Dirección de correo electrónico	vmca@vmware.com	vpxd.certmgmt.certs.cn.email
Localidad (Ciudad)	Palo Alto	vpxd.certmgmt.certs.cn.localityName
Nombre de unidad de organización	Ingeniería de VMware	vpxd.certmgmt.certs.cn.organizationalUnitName
Nombre de organización	VMware	vpxd.certmgmt.certs.cn.organizationName
Estado o provincia	California	vpxd.certmgmt.certs.cn.state

Tabla 3-5. Configuración de CSR ESXi (continuación)

Parámetro	Valor predeterminado	Opción avanzada
Cantidad de días en que el certificado es válido.	1825	vpxd.certmgmt.certs.daysValid
Umbral estricto para la caducidad de los certificados. vCenter Server activa una alarma roja cuando se alcanza este umbral.	30 días	vpxd.certmgmt.certs.hardThreshold
Intervalo de medición de las comprobaciones de validez de certificados de vCenter Server.	5 días	vpxd.certmgmt.certs.pollIntervalDays
Umbral flexible para la caducidad de los certificados. vCenter Server activa un evento cuando se alcanza este umbral.	240 días	vpxd.certmgmt.certs.softThreshold
Modo en que los usuarios de vCenter Server determinan si los certificados existentes deben reemplazarse. Cambie este modo para conservar los certificados durante la actualización. Consulte Certificados y actualizaciones de hosts ESXi.	vmca También puede especificar el modo de huella digital o personalizado. Consulte Cambiar el modo de certificado de ESXi.	modo de vpxd.certmgmt.

Cambiar la configuración predeterminada de certificados de ESXi

Cuando se agrega un host ESXi a un sistema vCenter Server, vCenter Server envía una solicitud de firma de certificado (CSR, Certificate Signing Request) para el host en VMCA. Se puede cambiar parte de la configuración predeterminada en la CSR a través de la configuración avanzada de vCenter Server en vSphere Client.

Consulte la tabla anterior para obtener una lista de los ajustes predeterminados. Algunos de los valores predeterminados no se pueden cambiar.

Procedimiento

1 En vSphere Client, seleccione el sistema vCenter Server que administra los hosts.

2 Haga clic en **Configurar** y en **Configuración avanzada**.

3 Haga clic en **Editar configuración**.

4 Haga clic en el icono **Filtrar** en la columna Nombre; en el cuadro Filtrar, escriba **`vpxd.certmgmt`** para que se muestren únicamente los parámetros de administración de certificados.

5 Cambie el valor de los parámetros actuales para cumplir con la directiva de la empresa y haga clic en **Guardar**.

La próxima vez que se agregue un host a vCenter Server, la nueva configuración se utilizará en la CSR que vCenter Server envía a VMCA y en el certificado que se asigna al host.

Pasos siguientes

Los cambios en los metadatos de los certificados solo afectan a los nuevos certificados. Si desea cambiar los certificados de los hosts que ya se administran mediante el sistema vCenter Server, desconecte los hosts y vuelva a conectarlos, o bien renueve los certificados.

Ver la información de caducidad de certificados de hosts ESXi

En los hosts ESXi que están en modo VMCA o modo personalizado, se pueden ver los detalles de los certificados desde vSphere Client. La información de los certificados te permite determinar si alguno de los certificados está a punto de caducar. También puede utilizar esta información para depurar problemas de certificados.

No se puede ver la información del estado de los certificados de los hosts ESXi que están en modo de huella digital. Puede ver información de varios hosts ESXi o de un solo host ESXi. La visualización de varios hosts solo muestra la información de la fecha de Certificado válido hasta.

Procedimiento

1 Inicie sesión en vCenter Server mediante vSphere Client.

2 Examine la lista de inventario y seleccione la instancia de vCenter Server.

3 Obtenga la información del certificado.

Host único o varios hosts	Pasos
Individual	a Desplácese hasta el host ESXi. b Haga clic en **Configurar**. c En **Sistema**, haga clic en **Certificado**.
Varios	a Seleccione **Hosts y clústeres > Hosts**. De forma predeterminada, la pantalla Hosts no incluye el estado de los certificados. b Para mostrar u ocultar columnas, haga clic en **Administrar columnas**. c Seleccione la casilla **Certificado válido hasta** y desplácese hacia la derecha si es necesario para ver la columna agregada. La información del certificado muestra la fecha de caducidad del certificado. d (Opcional) Anule la selección de otras columnas para que le sea más fácil ver lo que le interesa.

4 Revise la información del certificado.

La siguiente información solo está disponible en la vista de host único.

Campo	Descripción
Asunto	El asunto usado durante la generación del certificado.
Emisor	El emisor del certificado.
Válido desde	La fecha en la que se generó el certificado.
Válido hasta	La fecha en la que caduca el certificado.
Estado	El estado del certificado, que puede ser: **Bueno** Funcionamiento normal. **Por caducar** El certificado caducará pronto. **Por caducar en breve** El certificado caducará en ocho meses o menos (valor predeterminado). **Caducidad inminente** El certificado caducará en dos meses o menos (valor predeterminado). **Caducó** El certificado no es válido porque ya caducó.

Nota Si un host se agrega a vCenter Server o se vuelve a conectar después de una desconexión, vCenter Server renueva el certificado siempre y cuando el estado sea Caducado, En caducidad, Por caducar o Caducidad inminente. El estado es Expiring si el certificado es válido durante menos de ocho meses, Expiring shortly si el certificado es válido durante menos de dos meses y Expiration imminent si el certificado es válido durante menos de un mes.

Pasos siguientes

Renueve los certificados que estén por caducar. Consulte Renovar o actualizar de certificados de ESXi.

Renovar o actualizar de certificados de ESXi

Si utiliza VMware Certificate Authority (VMCA) para asignar certificados a los hosts, puede renovarlos desde vSphere Client. Si utiliza certificados de VMCA o certificados personalizados, puede actualizar todos los certificados del almacén de TRUSTED_ROOTS asociado con vCenter Server.

Puede utilizar vSphere Client para renovar los certificados de VMCA cuando estos estén a punto de caducar o si desea aprovisionar el host con un certificado nuevo por otros motivos. Si no renueva el certificado de VMCA antes de que caduque, desconectar el host y volver a conectarlo hace que vCenter Server renueve el certificado. La acción de volver a agregar el host a vCenter Server restablece la confianza y permite que vCenter Server emita el certificado renovado sin condiciones.

De forma predeterminada, vCenter Server renueva el certificado de VMCA de un host que tenga el estado Caducó, Caducidad inminente o Por caducar en breve cada vez que el host se agregue al inventario o se vuelva a conectar.

No se puede renovar un certificado de ESXi cuya fecha de caducidad sea posterior a la fecha de caducidad del certificado raíz de confianza. Por ejemplo, aunque la opción avanzada `vpxd.certmgmt.certs.daysValid` de ESXi esté establecida en cinco años y el certificado raíz de confianza caduque dentro de dos años, la fecha de caducidad del certificado de ESXi se limita a dos años.

Puede utilizar vSphere Client para insertar todos los certificados que se encuentran actualmente en el almacén de TRUSTED_ROOTS del almacén VECS de vCenter Server en el host ESXi. Utilice esta capacidad si necesita actualizar las raíces de confianza en un host ESXi. Esta capacidad existe para los certificados personalizados y de VMCA.

Requisitos previos

Compruebe lo siguiente:

- Si utiliza certificados de VMCA, el modo de certificación se establece en **vmca**.
- Si utiliza certificados personalizados, el modo de certificación se establece en **personalizado**.
- Los hosts ESXi están conectados al sistema vCenter Server.
- La sincronización de hora que se produce entre el sistema vCenter Server y los hosts ESXi es la adecuada.
- La resolución de DNS funciona entre el sistema vCenter Server y los hosts ESXi.
- Los certificados Trusted_Root y MACHINE_SSL_CERT del sistema vCenter Server son válidos y no han caducado. Consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/2111411.
- Los hosts ESXi no están en modo de mantenimiento.

Nota Si utiliza certificados personalizados y necesita renovarlos, vuelva a importar los certificados.

Procedimiento

1 Desplácese hasta el host en el inventario de vSphere Client.

2 Haga clic en **Configurar**.

3 En **Sistema**, haga clic en **Certificado**.

Puede ver los detalles del certificado del host seleccionado.

4 Seleccione la opción adecuada en función del tipo de certificado utilizado.

Opción	Descripción
Administrar con VMCA > Renovar	Recupera un certificado recién firmado desde VMCA para el host.
Administrar con VMCA > Actualizar certificados de CA **o** **Administrar con CA externa > Actualizar certificados de CA**	Envía todos los certificados del almacén TRUSTED_ROOTS del almacén vCenter Server VECS al host.

Cambiar el modo de certificado de ESXi

Utilice VMware Certificate Authority (VMCA) para aprovisionar los hosts ESXi en su entorno, a menos que la directiva corporativa exija que se usen certificados personalizados. En ese caso, para usar certificados personalizados con otra entidad de certificación raíz, edite el ajuste de vCenter Server avanzado, `vpxd.certmgmt.mode`. Tras aplicar el cambio, los hosts dejarán de aprovisionarse automáticamente con certificados de VMCA cuando se actualicen los certificados. y usted será responsable de administrar los certificados del entorno.

Puede utilizar la configuración avanzada de vCenter Server para cambiar al modo de huella digital o al modo de entidad de certificación personalizada. Utilice el modo de huella digital únicamente como opción de reserva.

Procedimiento

1 En vSphere Client, seleccione el sistema vCenter Server que administra los hosts.

2 Haga clic en **Configurar** y en Configuración, haga clic en **Configuración avanzada**.

3 Haga clic en **Editar configuración**.

4 Haga clic en el icono **Filtrar** en la columna Nombre; en el cuadro Filtrar, escriba **`vpxd.certmgmt`** para que se muestren únicamente los parámetros de administración de certificados.

Nota Las opciones disponibles son **vmca**, **personalizado** y **huella digital**.

5 Cambie el valor de `vpxd.certmgmt.mode` a **personalizado** si desea administrar sus propios certificados o a **huella digital** si desea utilizar el modo de huella digital temporalmente. Después, haga clic en **Guardar**.

Reemplazar el certificado de ESXi predeterminado por un certificado personalizado

La directiva de seguridad de su empresa puede requerir que reemplace el certificado SSL predeterminado de ESXi por un certificado firmado por una entidad de certificación (CA) externa en todos los hosts.

De forma predeterminada, los componentes de vSphere utilizan el certificado firmado por VMCA y la clave que se crean durante la instalación. Si elimina el certificado firmado por VMCA de forma accidental, quite el host de su sistema vCenter Server y vuelva a agregarlo. Al agregar el host, vCenter Server solicita un certificado nuevo de VMCA y aprovisiona el host con este certificado.

Puede reemplazar los certificados firmados por VMCA por certificados de una entidad de certificación de confianza, ya sea una CA comercial o una CA organizativa, si la directiva de su empresa lo requiere.

Puede reemplazar los certificados predeterminados por certificados personalizados mediante vSphere Client o la CLI.

Nota También puede utilizar los objetos administrados `vim.CertificateManager` y `vim.host.CertificateManager` en vSphere Web Services SDK. Consulte la documentación de vSphere Web Services SDK.

Antes de reemplazar el certificado, debe actualizar el almacén TRUSTED_ROOTS de VECS en el sistema vCenter Server que administra el host, para que vCenter Server y el host ESXi tengan una relación de confianza.

Nota Si va a reemplazar certificados SSL en un host ESXi que forma parte de un clúster de vSAN, siga los pasos que se indican en el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/56441.

Requisitos para las solicitudes de firma del certificado de ESXi para certificados personalizados

Utilice una CSR con estas características:

- Tamaño de clave: de 2048 bits (mínimo) a 8192 bits (máximo) (formato codificado PEM)
- Formato PEM. VMware admite PKCS8 y PKCS1 (claves RSA). Cuando se agregan claves a VECS, se convierten en PKCS8.
- x509 versión 3
- Para los certificados raíz, la extensión CA se debe establecer en true y el signo cert debe estar en la lista de requisitos.
- SubjectAltName debe contener DNS Name=<machine_FQDN>.
- Formato CRT
- Contiene los siguientes usos de claves: firma digital, cifrado de clave

- Hora de inicio de un día anterior a la hora actual.
- CN (y SubjectAltName) establecidos con el nombre de host (o dirección IP) que el host ESXi tiene en el inventario de vCenter Server.

Nota El certificado FIPS de vSphere solo valida los tamaños 2048 y 3072 de clave RSA. Consulte Consideraciones al utilizar FIPS.

vSphere no admite los siguientes certificados.

- Certificados con comodines.
- No se admiten los algoritmos md2WithRSAEncryption, md5WithRSAEncryption, RSASSA-PSS, dsaWithSHA1, ecdsa_with_SHA1 y sha1WithRSAEncryption.

Para generar la CSR mediante vSphere Client, consulte Generar una solicitud de firma del certificado para un certificado personalizado mediante vSphere Client.

Para obtener información sobre cómo generar la CSR mediante la CLI, consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/2113926.

Qué leer a continuación

- Generar una solicitud de firma del certificado para un certificado personalizado mediante vSphere Client

  A partir de vSphere 8.0 Update 3, puede utilizar vSphere Client para generar una solicitud de firma del certificado (CSR) para el certificado SSL de ESXi y reemplazar el certificado una vez que esté listo.
- Reemplazar el certificado predeterminado por un certificado personalizado mediante vSphere Client

  Puede reemplazar los certificados de ESXi firmados por VMCA predeterminados con certificados personalizados de vSphere Client.
- Reemplazar el certificado y de la clave predeterminados de ESXi Shell

  Puede reemplazar los certificados firmados por VMCA predeterminados de ESXi en ESXi Shell.
- Reemplazar el certificado predeterminado mediante el método PUT de HTTPS

  Puede usar aplicaciones de terceros para cargar certificados y claves. Las aplicaciones que admiten las operaciones del método PUT de HTTPS funcionan con la interfaz de HTTPS incluida en ESXi.
- Actualizar el almacén TRUSTED_ROOTS de vCenter Server (certificados personalizados)

  Si configura los hosts ESXi para usar certificados personalizados, debe actualizar el almacén `TRUSTED_ROOTS` en el sistema vCenter Server que administra los hosts.

Generar una solicitud de firma del certificado para un certificado personalizado mediante vSphere Client

A partir de vSphere 8.0 Update 3, puede utilizar vSphere Client para generar una solicitud de firma del certificado (CSR) para el certificado SSL de ESXi y reemplazar el certificado una vez que esté listo.

Requisitos previos

Cambie el modo de certificación a **personalizado**. Consulte Cambiar el modo de certificado de ESXi. Al cambiar el modo, vSphere Client activará el menú desplegable **Administrar con CA externa** para que pueda generar la solicitud de firma del certificado.

Advertencia Al generar una solicitud de firma del certificado, se genera una clave privada nueva. No genere otra solicitud de firma del certificado durante el proceso de reemplazo de certificados. Si lo hace, la CSR generada anteriormente y el certificado posterior dejarán de ser válidos.

Procedimiento

1. Desplácese hasta el host en el inventario de vSphere Client.
2. Haga clic en **Configurar**.
3. En **Sistema**, haga clic en **Certificado**.
4. En el menú desplegable **Administrar con una CA externa**, seleccione **Generar CSR mediante IP** o **Generar CSR mediante FQDN**.

   vCenter Server identifica la opción que se utilizó anteriormente para generar el certificado en el host ESXi.
5. Seleccione **Copiar en el portapapeles** o **Descargar**, en función de cómo desee generar la solicitud de firma del certificado.

Pasos siguientes

Ahora puede enviar la CSR a la entidad de certificación o utilizar la CSR para generar el certificado de forma interna.

Reemplazar el certificado predeterminado por un certificado personalizado mediante vSphere Client

Puede reemplazar los certificados de ESXi firmados por VMCA predeterminados con certificados personalizados de vSphere Client.

Al importar el certificado personalizado, asegúrese de lo siguiente:

- Agregue toda la cadena de certificados de CA antes de continuar con el reemplazo.
- Asegúrese de proporcionar el certificado de CA correcto para su entorno. El proceso de importación y reemplazo no realiza la comprobación del certificado que se utiliza.

- Asegúrese de que no haya ningún hash SHA1 en la cadena de certificados. SHA1 no es compatible.
- Agregue la CA raíz a VECS antes de continuar. De lo contrario, el host se desconectará inmediatamente después del reemplazo del certificado.

Requisitos previos

- Genere la solicitud de firma del certificado y envíela a la entidad de certificación. Consulte Generar una solicitud de firma del certificado para un certificado personalizado mediante vSphere Client.
- Cuando la entidad de certificación devuelva el certificado, guárdelo en los hosts ESXi.
- Asegúrese de que el modo de certificación de ESXi esté establecido en **personalizado**. Consulte Cambiar el modo de certificado de ESXi.
- Actualice el almacén raíz de confianza. Consulte Actualizar el almacén TRUSTED_ROOTS de vCenter Server (certificados personalizados).

Procedimiento

1 Desplácese hasta el host en el inventario de vSphere Client.

2 Haga clic en **Configurar**.

3 En **Sistema**, haga clic en **Certificado**.

4 En el menú desplegable **Administrar con CA externa**, seleccione **Importar y reemplazar**.

5 Seleccione la opción de reemplazo.

Opción	Descripción
Reemplazar con un certificado de CA externa donde la CSR se genera mediante ESXi (clave privada integrada)	Utilice esta opción si generó la CSR en ESXi, en cuyo caso la clave privada se almacena en ESXi.
Reemplazar con un certificado de CA externa donde la CSR se genera desde una entidad de certificación (requiere una clave privada)	Utilice esta opción si envió la CSR a una entidad de certificación de terceros y recibió de nuevo el certificado y la clave privada.

6 Haga clic en **Siguiente**.

7 Busque el certificado, o el certificado y la clave privada.

8 Revise la información y, a continuación, haga clic en **Importar y reemplazar**.

Resultados

El certificado personalizado reemplaza el certificado actual.

Reemplazar el certificado y de la clave predeterminados de ESXi Shell

Puede reemplazar los certificados firmados por VMCA predeterminados de ESXi en ESXi Shell.

Requisitos previos

- Si desea usar certificados firmados por una entidad de certificación (CA) externa, genere la solicitud de certificación, envíela a la entidad de certificación y almacene los certificados en cada host ESXi.
- De ser necesario, habilite ESXi Shell o el tráfico SSH desde vSphere Client.
- Todas las transferencias de archivos y demás comunicaciones se realizan en una sesión de HTTPS segura. El usuario que se usa para autenticar la sesión debe tener el privilegio **Host.Configuración.Configuración avanzada** en el host.

Nota Antes de reemplazar los certificados, actualice el almacén de TRUSTED_ROOTS de vCenter Server. Consulte Actualizar el almacén TRUSTED_ROOTS de vCenter Server (certificados personalizados).

Procedimiento

1 Inicie sesión en ESXi Shell, ya sea directamente desde la DCUI o desde un cliente de SSH, como un usuario con privilegios de administrador.

2 En el directorio `/etc/vmware/ssl`, cambie el nombre de los certificados existentes con los siguientes comandos.

```
mv rui.crt orig.rui.crt
mv rui.key orig.rui.key
```

3 Copie los certificados que desea utilizar en `/etc/vmware/ssl`.

4 Cambie el nombre del certificado nuevo y de la clave por `rui.crt` y `rui.key`.

5 Después de instalar el certificado nuevo, reinicie el host.

Como alternativa, puede colocar el host en modo de mantenimiento, instalar el certificado nuevo, utilizar la interfaz de usuario de la consola directa (DCUI) para reiniciar los agentes de administración y, a continuación, establecer el host para que salga del modo de mantenimiento.

Reemplazar el certificado predeterminado mediante el método PUT de HTTPS

Puede usar aplicaciones de terceros para cargar certificados y claves. Las aplicaciones que admiten las operaciones del método PUT de HTTPS funcionan con la interfaz de HTTPS incluida en ESXi.

Requisitos previos

- Si desea usar certificados firmados por una entidad de certificación (CA) externa, genere la solicitud de certificación, envíela a la entidad de certificación y almacene los certificados en cada host ESXi.
- De ser necesario, habilite ESXi Shell o el tráfico SSH desde vSphere Client.

- Todas las transferencias de archivos y demás comunicaciones se realizan en una sesión de HTTPS segura. El usuario que se usa para autenticar la sesión debe tener el privilegio **Host.Configuración.Configuración avanzada** en el host.

Nota Antes de reemplazar los certificados, actualice el almacén de TRUSTED_ROOTS de vCenter Server. Consulte Actualizar el almacén TRUSTED_ROOTS de vCenter Server (certificados personalizados).

Procedimiento

1 Realice una copia de seguridad de los certificados actuales.

2 Configure la autenticación de acceso básica, en la que proporciona un nombre de usuario y una contraseña codificados en Base64, separados por dos puntos (:). Para obtener más información, consulte https://en.wikipedia.org/wiki/Basic_access_authentication.

3 En la aplicación de carga, procese cada archivo de la siguiente manera:

   a Abra el archivo.

   b Publique el archivo en una de estas ubicaciones.

Opción	Descripción
Certificados	`https://hostname/host/ssl_cert`
Claves	`https://hostname/host/ssl_key`

   Las ubicaciones `/host/ssl_cert` y `host/ssl_key` conducen a los archivos de certificado en `/etc/vmware/ssl`.

4 Reinicie el host.

   Como alternativa, puede colocar el host en modo de mantenimiento, instalar el certificado nuevo, utilizar la interfaz de usuario de la consola directa (DCUI) para reiniciar los agentes de administración y, a continuación, establecer el host para que salga del modo de mantenimiento.

Actualizar el almacén TRUSTED_ROOTS de vCenter Server (certificados personalizados)

Si configura los hosts ESXi para usar certificados personalizados, debe actualizar el almacén `TRUSTED_ROOTS` en el sistema vCenter Server que administra los hosts.

Requisitos previos

Reemplace los certificados de cada host por los certificados personalizados.

Nota Este paso no es necesario si el sistema vCenter Server también se ejecuta con certificados personalizados emitidos por la misma entidad de certificación que los instalados en los hosts ESXi.

Procedimiento

1. Para actualizar el almacén TRUSTED_ROOTS de vCenter Server mediante vSphere Client, consulte Agregar un certificado raíz de confianza al almacén de certificados mediante vSphere Client.
2. Para actualizar el almacén TRUSTED_ROOTS de vCenter Server mediante la interfaz de línea de comandos, inicie sesión en el shell de vCenter Server del sistema de vCenter Server que administra los hosts ESXi.
3. Para agregar los nuevos certificados al almacén `TRUSTED_ROOTS`, ejecute `dir-cli`, por ejemplo:

   ```
   /usr/lib/vmware-vmafd/bin/dir-cli trustedcert publish --cert path_to_RootCA
   ```

4. Cuando se le solicite, proporcione las credenciales de administrador de Single Sign-On.
5. Si los certificados personalizados son emitidos por una entidad de certificación intermedia, también debe agregar esta entidad al almacén `TRUSTED_ROOTS` en vCenter Server, por ejemplo:

   ```
   /usr/lib/vmware-vmafd/bin/dir-cli trustedcert publish --cert path_to_intermediateCA
   ```

Pasos siguientes

Establezca el modo de certificación en Personalizado. Si el modo de certificación es VMCA (el modo predeterminado) y ejecuta una actualización de certificados, los certificados firmados por VMCA reemplazan los certificados personalizados. Consulte Cambiar el modo de certificado de ESXi.

Convertir a Auto Deploy en una autoridad de certificación subordinada

De manera predeterminada, el servidor Auto Deploy aprovisiona cada host con certificados que estén firmados por VMware Certificate Authority (VMCA). Es posible configurar el servidor Auto Deploy para que aprovisione todos los hosts con certificados personalizados que no estén firmados por VMCA. En ese caso, el servidor Auto Deploy se transforma en una entidad de certificación subordinada a la entidad de certificación externa.

Requisitos previos

- Solicite a la CA un certificado. El certificado debe cumplir con estos requisitos.
  - Tamaño de clave: de 2048 bits (mínimo) a 8192 bits (máximo) (formato codificado PEM)
  - Formato PEM. VMware admite PKCS8 y PKCS1 (claves RSA). Cuando se agregan claves a VECS, se convierten en PKCS8.
  - x509 versión 3
  - Para los certificados raíz, la extensión CA se debe establecer en true y el signo cert debe estar en la lista de requisitos.

- SubjectAltName debe contener DNS Name=<machine_FQDN>.
- Formato CRT
- Contiene los siguientes usos de claves: firma digital, cifrado de clave
- Hora de inicio de un día anterior a la hora actual.
- CN (y SubjectAltName) establecidos con el nombre de host (o dirección IP) que el host ESXi tiene en el inventario de vCenter Server.

Nota El certificado FIPS de vSphere solo valida los tamaños 2048 y 3072 de clave RSA. Consulte Consideraciones al utilizar FIPS.

- Asigne un nombre para el certificado y los archivos de claves `rbd-ca.crt` y `rbd-ca.key`.

Procedimiento

1 Realice una copia de seguridad de los certificados de ESXi predeterminados.

Los certificados están en el directorio `/etc/vmware-rbd/ssl/`.

2 Detenga el servicio de vSphere Authentication Proxy.

Herramienta	Pasos
Interfaz de administración de vCenter Server	a En un explorador web, vaya a la interfaz de administración de vCenter Server, https://*dirección-IP-o-FQDN-de-vCenter*:5480. b Inicie sesión como raíz. La contraseña raíz predeterminada es la que estableció al implementar vCenter Server. c Haga clic en **Servicios** y en **VMware vSphere Authentication Proxy**. d Haga clic en **Detener**.
CLI	`service-control --stop vmcam`

3 En el sistema donde se ejecuta el servicio de Auto Deploy, reemplace `rbd-ca.crt` y `rbd-ca.key` en `/etc/vmware-rbd/ssl/` por el certificado personalizado y los archivos de claves.

4 En el sistema donde se ejecuta el servicio de Auto Deploy, ejecute el siguiente comando a fin de actualizar el almacén TRUSTED_ROOTS en VMware Endpoint Certificate Store (VECS) para utilizar los nuevos certificados.

```
/usr/lib/vmware-vmafd/bin/dir-cli trustedcert publish --cert /etc/vmware-rbd/ssl/rbd-ca.crt
/usr/lib/vmware-vmafd/bin/vecs-cli force-refresh
```

5 Cree un archivo `castore.pem` que incluya el contenido del almacén TRUSTED_ROOTS y coloque el archivo en el directorio `/etc/vmware-rbd/ssl/`.

En el modo personalizado, usted es responsable de mantener este archivo.

6 Cambie el modo de certificación de ESXi del sistema de vCenter Server a **custom**.

   Consulte Cambiar el modo de certificado de ESXi.

7 Reinicie el servicio de vCenter Server e inicie el servicio de Auto Deploy.

Resultados

La próxima vez que aprovisione un host que esté configurado para usar Auto Deploy, el servidor Auto Deploy generará un certificado. El servidor Auto Deploy utiliza el certificado raíz que agregó al almacén TRUSTED_ROOTS.

Nota Si tiene problemas con Auto Deploy después de reemplazar el certificado, consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/2000988.

Usar certificados personalizados con Auto Deploy

En vSphere 8.0 o versiones posteriores, el servidor Auto Deploy se puede configurar para aprovisionar los hosts ESXi con certificados personalizados que estén firmados por una entidad de certificación (CA) externa o por su propia entidad de certificación interna. De manera predeterminada, el servidor Auto Deploy aprovisiona los hosts ESXi con certificados firmados por VMware Certificate Authority (VMCA).

Antes de vSphere 8.0, las opciones para administrar certificados con Auto Deploy incluyen:

- Usar vCenter Server y la autoridad de certificación VMware Certificate Authority integrada (la opción predeterminada).
- Convertir a Auto Deploy en una entidad de certificación subordinada de una CA externa. En este caso, la clave SSL de Auto Deploy firma los certificados.

En vSphere 8.0 o versiones posteriores, puede cargar certificados personalizados en Auto Deploy que estén firmados por una entidad de certificación externa o por su propia entidad de certificación interna. Auto Deploy asocia el certificado personalizado con la dirección MAC o el UUID del BIOS del host ESXi. Cada vez que se inicia un host de Auto Deploy, Auto Deploy comprueba si hay un certificado personalizado. Si Auto Deploy encuentra un certificado personalizado, lo utiliza en lugar de generar uno a través de VMCA.

Los pasos de alto nivel de esta tarea incluyen:

1 Generar la solicitud de certificado personalizada para una entidad de certificación externa o para su propia entidad de certificación interna.

2 Obtener el certificado personalizado firmado (clave y certificado) y almacenarlo en local.

3 Si utiliza una entidad de certificación externa y, si no lo hizo antes, asegurarse de que el certificado raíz de su CA esté cargado en el almacén TRUSTED_ROOTS de la instancia de vCenter Server.

4 Cargar el certificado personalizado en Auto Deploy y asociar el certificado con la dirección MAC o el UUID del BIOS de un host ESXi.

5 Iniciar el host ESXi.

Cuando se asigna un certificado personalizado a un host ESXi, Auto Deploy inserta el certificado en el host en el siguiente inicio que se haga desde Auto Deploy.

Tenga en cuenta las siguientes consideraciones al utilizar certificados personalizados y Auto Deploy.

- Debe usar los cmdlets `Add-CustomCertificate`, `Remove-CustomCertificate` y `List-CustomCertificate` de PowerCLI para administrar los certificados personalizados que se utilizan con Auto Deploy. La capacidad para administrar certificados personalizados no está disponible en vSphere Client.
- Para actualizar un certificado personalizado que se utiliza para Auto Deploy, debe volver a ejecutar el cmdlet `Add-CustomCertificate`.
- Asegúrese de examinar el certificado personalizado en busca de posibles errores. Auto Deploy solo comprueba que el certificado personalizado cumpla con los estándares del certificado X.509 y que el umbral de caducidad del certificado esté configurado en al menos 240 días. Auto Deploy no realiza ninguna otra validación o comprobación de certificados. Para cambiar el umbral del certificado, puede ejecutar el cmdlet `Set-DeployOption -Key certificate-refresh-threshold`.
- Si posteriormente elimina un certificado personalizado de un host ESXi mediante el cmdlet `Remove-CustomCertificate`, debe reiniciar el host para que el cambio surta efecto.

Para obtener más información sobre certificados personalizados y Auto Deploy, consulte la documentación de *Instalar y configurar VMware ESXi*.

Requisitos previos

Compruebe que dispone de lo siguiente:

- Solicite un certificado a la entidad de certificación. El certificado debe cumplir con estos requisitos.
  - Tamaño de clave: de 2048 bits (mínimo) a 8192 bits (máximo) (formato codificado PEM)
  - Formato PEM. VMware admite PKCS8 y PKCS1 (claves RSA). Cuando se agregan claves a VECS, se convierten en PKCS8.
  - x509 versión 3
  - Formato CRT
  - Extensión de CA establecida en true
  - Uso de claves de firma de certificado
  - Hora de inicio de un día anterior a la hora actual

  Nota El certificado FIPS de vSphere solo valida los tamaños 2048 y 3072 de clave RSA. Consulte Consideraciones al utilizar FIPS.

- Dirección MAC del host ESXi o UUID del BIOS. Evalúe qué enfoque es el más adecuado para su entorno. El UUID del BIOS es más estable y está sujeto a menos cambios que la dirección MAC. Si cambia los adaptadores de red en un host ESXi, cambia la dirección MAC. Sin embargo, es posible que conozca mejor la dirección MAC para trabajar con ella y que sea más fácil de obtener que el UUID del BIOS.
- Al menos la versión 12.6.0 de PowerCLI. Para obtener más información sobre los cmdlets de Auto Deploy PowerCLI, consulte el tema "Descripción general de cmdlets de Auto Deploy PowerCLI" en la documentación de *Instalar y configurar VMware ESXi*.

Asegúrese de disponer de los siguientes privilegios:

- Agregar certificado personalizado: **Auto Deploy.Regla.Crear**
- Obtener información del certificado personalizado: **Sistema.Lectura**

Procedimiento

1 Genere la solicitud de certificado.

   a Con los requisitos enumerados anteriormente para la solicitud del certificado, cree un archivo de configuración (.cfg).

   b Para generar un archivo CSR y un archivo de clave, ejecute el comando `openssl req`, pasando el archivo de configuración (.cfg).

   Por ejemplo:

   ```
   openssl req -new -config custom_cert.cfg -days 4200 -sha256 -keyout rui.key -out
   rui.csr
   ```

   En este comando:

   - `-new` genera una nueva solicitud de certificado.
   - `-config custom_cert.cfg` especifica el archivo .cfg personalizado.
   - `-days 4200` especifica 4200 días durante los cuales se puede certificar el certificado.
   - `-sha256` especifica el resumen del mensaje con el que firmar la solicitud.
   - `-keyout rui.key` especifica el archivo en el que se debe escribir la clave privada recién creada.
   - `-out rui.csr` especifica el archivo de salida en el que se va a escribir.

2 Envíe la solicitud de certificado a la entidad de certificación externa o, si firma sus propios certificados, ejecute el comando `openssl x509 -req` para generar el certificado personalizado a partir del archivo `rui.csr`.

Por ejemplo:

```
openssl x509 -req -in rui.csr -CA "/etc/vmware-rbd/ssl/rbd-ca.crt" -CAkey \
"/etc/vmware-rbd/ssl/rbd-ca.key" -extfile \
openssl.cfg -extensions x509 -CAserial "/etc/vmware-rbd/ssl/rbd-ca.srl" -days \
4200 -sha256 -out signed_rui.crt
```

En este comando:

- `-in rui.csr` especifica el archivo de entrada.
- `-CA "/etc/vmware-rbd/ssl/rbd-ca.crt"` especifica el directorio que se utilizará para la verificación del certificado del servidor.
- `-CAkey "/etc/vmware-rbd/ssl/rbd-ca.key"` establece la clave privada de la entidad de certificación con la que se va a firmar un certificado.
- `-extfile openssl.cfg` especifica un archivo de configuración opcional adicional en el que se van a leer las extensiones de certificado.
- `-extensions x509` especifica que se deben usar extensiones de certificado x509.
- `-CAserial "/etc/vmware-rbd/ssl/rbd-ca.srl"` utiliza el número de serie de `rbd-ca.srl` para firmar un certificado.
- `-days 4200` especifica 4200 días durante los cuales se puede certificar el certificado.
- `-sha256` especifica el resumen del mensaje con el que firmar la solicitud.
- `-out signed_rui.crt` especifica el archivo de salida en el que se va a escribir.

3 (opcional) Si no cargó previamente el certificado de su entidad de certificación de firma en el almacén TRUSTED_ROOTS dentro de VMware Endpoint Certificate Store (VECS), realice los siguientes pasos en la instancia de vCenter Server donde se ejecuta el servicio de Auto Deploy.

   a Con una herramienta como WinSCP, copie el certificado en la instancia de vCenter Server.

   b Inicie sesión en la instancia de vCenter Server mediante SSH y ejecute el siguiente comando.

   ```
   /usr/lib/vmware-vmafd/bin/dir-cli trustedcert publish --cert path_to_ca_certificate
   ```

4 Obtenga la dirección MAC del host ESXi o el UUID del BIOS.

5 Realice los siguientes pasos para agregar el certificado personalizado a Auto Deploy.

a Para conectarse a vCenter Server, ejecute el cmdlet `Connect-VIServer`.

```
Connect-VIServer -server VC_ip_address -User administrator_user -Password 'password'
```

b (opcional) Para ver los certificados personalizados existentes, ejecute el cmdlet `Get-CustomCertificates`.

La primera vez que agregue certificados personalizados, no verá ningún certificado devuelto mediante este cmdlet.

c Para asociar el certificado personalizado al host ESXi, ejecute el cmdlet `Add-CustomCertificate`.

```
Add-CustomCertificate -HostID [MAC_Address | BIOS_UUID] -Certificate
"path_to_custom_cert" -Key "path_to_custom_cert_key"
```

Puede especificar la dirección MAC o el UUID del BIOS del host. Auto Deploy carga el certificado personalizado en el host.

d Para comprobar que se cargó el certificado, ejecute el cmdlet `Get-CustomCertificates`.

Verá resultados similares al siguiente:

```
Name:     CustomHostCert-1
CertificateId:      1
HostId:             02:08:b0:8e:18:a2
ExpirationTime: 1   2/28/2033 10:45:50 AM
TimeCreated:        9/29/2022 7:40:28 AM
LastModified:       9/29/2022 7:40:28 AM
AssociatedHostName:
```

`AssociatedHostName` está en blanco por ahora. Después de iniciar el host, el resultado reflejará el nombre del host ESXi asociado al certificado personalizado.

6 Inicie el host ESXi.

7 Para comprobar que el certificado personalizado esté asociado a la instancia de vCenter Server, vuelva a ejecutar el cmdlet `Get-CustomCertificates`.

Verá un resultado similar al siguiente.

```
Name:     CustomHostCert-1
CertificateId:      1
HostId:             02:08:b0:8e:18:a2
ExpirationTime: 1   2/28/2033 10:45:50 AM
TimeCreated:        9/29/2022 7:40:28 AM
LastModified:       9/29/2022 7:40:28 AM
AssociatedHostName: host1.example.com
```

Ahora `AssociatedHostName` contiene el nombre del host ESXi.

Restaurar archivos de clave y certificado de ESXi cuando se produce un error en el reemplazo de certificados

Cuando se produce un error al reemplazar un certificado en un host ESXi, el sistema crea archivos de certificación `.bak` que puede utilizar para recuperar el estado anterior.

El certificado y la clave del host se encuentran en `/etc/vmware/ssl/rui.crt` y `/etc/vmware/ssl/rui.key`. Cuando se reemplaza un certificado de host mediante vSphere Client o el objeto administrado `vim.CertificateManager` de vSphere Web Services SDK, y se produce un error en el reemplazo, el sistema crea archivos `.bak` para los archivos de clave y certificado anteriores.

Cuando se produce un error en el reemplazo de certificados, puede restaurar certificados anteriores copiando los archivos `.bak` en los archivos de certificados y claves actuales.

Personalizar la seguridad del host ESXi

Puede personalizar muchos de los ajustes de seguridad fundamentales para el host ESXi mediante los paneles Firewall, Servicios y Perfil de seguridad, disponibles en vSphere Client. El perfil de seguridad es especialmente útil para la administración de un host único. Si debe administrar varios hosts, considere utilizar una de las CLI o los SDK de VMware y automatizar las tareas de personalización.

Configurar el firewall de ESXi

ESXi incluye un firewall que está habilitado de forma predeterminada. En el momento de realizar la instalación, el firewall de ESXi se configura para bloquear el tráfico entrante y saliente, excepto el tráfico de los servicios que están habilitados en el perfil de seguridad del host. El firewall se administra mediante vSphere Client, la CLI y la API.

Al abrir puertos en el firewall, tenga en cuenta que el acceso no restringido a los servicios que se ejecutan en un host ESXi pueden exponer un host a ataques externos y acceso no autorizado. Para reducir el riesgo, configure el firewall de ESXi para que permita el acceso solo desde redes autorizadas.

Nota El firewall también permite pings del protocolo Control Message Protocol (ICMP) y la comunicación con los clientes DHCP y DNS (solo UDP).

Es posible administrar puertos de firewall de ESXi de la siguiente manera:

- Utilice las opciones **Configurar > Firewall** para cada host en vSphere Client. Consulte Administrar la configuración del firewall de ESXi.
- Utilice los comandos ESXCLI en la línea de comandos o en los scripts. Consulte Usar comandos de firewall ESXCLI para configurar el comportamiento de ESXi.
- Utilice un VIB si el puerto que desea abrir no está incluido en el perfil de seguridad.

Para instalar el VIB personalizado, se debe cambiar el nivel de aceptación del host ESXi a CommunitySupported.

Nota Si se contacta con el soporte técnico de VMware para investigar un problema en un host ESXi con un VIB CommunitySupported instalado, el soporte de VMware puede solicitarle que desinstale este VIB. Dicha solicitud es un paso de solución de problemas para determinar si ese VIB está relacionado con el problema que se investiga.

El comportamiento del conjunto de reglas del cliente NFS (`nfsClient`) es diferente a otros conjuntos de reglas. Cuando el conjunto de reglas del cliente NFS está habilitado, todos los puertos TCP salientes están abiertos para los hosts de destino que se incluyen en la lista de direcciones IP permitidas. Consulte Comportamiento de firewall del cliente NFS para obtener más información.

Administrar la configuración del firewall de ESXi

Puede configurar conexiones entrantes o salientes en el firewall para un servicio o un agente de administración desde vSphere Client o en la línea de comandos.

Esta tarea describe cómo utilizar la instancia de vSphere Client para configurar los ajustes de firewall de ESXi. Se pueden utilizar comandos de ESXi Shell o ESXCLI en la línea de comandos para configurar ESXi para automatizar la configuración del firewall. Consulte Usar comandos de firewall ESXCLI para configurar el comportamiento de ESXi para ver ejemplos del uso de ESXCLI para manipular firewalls y reglas de firewall.

Nota Si hay distintos servicios con reglas de puerto superpuestas, es posible que se activen otros servicios de forma implícita al habilitar un servicio. Para evitar este problema, se pueden especificar qué direcciones IP tienen permiso para acceder a cada servicio en el host.

Procedimiento

1. Inicie sesión en vCenter Server mediante vSphere Client.
2. Desplácese hasta el host en el inventario.
3. En **Sistema**, haga clic en **Configurar** y, a continuación, en **Firewall**.

   Para alternar entre conexiones entrantes y salientes, haga clic en **Entrante** y **Saliente**.
4. En la sección Firewall, haga clic en **Editar**.
5. Seleccione uno de los grupos de servicios: **Sin agrupar**, **Shell seguro** y **Protocolo de administración de red simple**.
6. Seleccione los conjuntos de reglas que se van a activar o anule la selección de la casilla de los conjuntos de reglas que se van a desactivar.
7. En algunos servicios, también puede administrar detalles del servicio; para ello, desplácese hasta **Configurar > Sistema > Servicios**.

   Para obtener más información sobre la forma de iniciar, detener y reiniciar los servicios, consulte Activar o desactivar un servicio de ESXi.

8 Para algunos servicios, se pueden especificar explícitamente las direcciones IP para las que se permiten conexiones.

Consulte Agregar direcciones IP permitidas para un host ESXi.

9 Haga clic en **Aceptar**.

Agregar direcciones IP permitidas para un host ESXi

De forma predeterminada, el firewall de cada servicio permite el acceso a todas las direcciones IP. Para restringir el tráfico, cambie cada servicio para permitir el tráfico solo desde la subred de administración. También puede anular la selección de algunos servicios si el entorno no los usa.

Para actualizar la lista de direcciones IP permitidas para un servicio, puede utilizar vSphere Client, ESXCLI o PowerCLI. Esta tarea describe cómo utilizar vSphere Client. Consulte el tema con el título "Administrar ESXi Firewall" en la documentación de *Conceptos y ejemplos de ESXCLI* para obtener instrucciones sobre cómo usar ESXCLI.

Procedimiento

1 Inicie sesión en vCenter Server mediante vSphere Client.

2 Desplácese hasta el host ESXi.

3 En **Sistema**, haga clic en **Configurar** y, a continuación, en **Firewall**.

Para alternar entre conexiones entrantes y salientes, haga clic en **Entrante** y **Saliente**.

4 En la sección Firewall, haga clic en **Editar**.

5 Seleccione uno de los tres grupos de servicios: **Sin agrupar**, **Shell seguro** y **Protocolo de administración de red simple**.

6 Para mostrar la sección Direcciones IP permitidas, amplíe un servicio.

7 En la sección Direcciones IP permitidas, desactive la casilla **Permitir conexiones desde cualquier dirección IP** e introduzca las direcciones IP de las redes que tienen permiso para conectarse al host.

Separe las direcciones IP con comas. Puede utilizar los siguientes formatos de dirección:

- 192.168.0.0/24
- 192.168.1.2, 2001::1/64
- fd3e:29a6:0a81:e478::/64

8 Asegúrese de que el servicio esté seleccionado.

9 Haga clic en **Aceptar**.

10 Compruebe el cambio en la columna **Direcciones IP permitidas** para el servicio.

Puertos de firewall entrantes y salientes para hosts de ESXi

Abra y cierre los puertos de firewall de cada servicio mediante vSphere Client o VMware Host Client.

ESXi incluye un firewall que está habilitado de forma predeterminada. En el momento de realizar la instalación, el firewall de ESXi se configura para bloquear el tráfico entrante y saliente, excepto el tráfico de los servicios que están habilitados en el perfil de seguridad del host. Para obtener la lista de los puertos y protocolos compatibles en el firewall de ESXi, consulte la herramienta VMware Ports and Protocols™ en https://ports.vmware.com/.

La herramienta VMware Ports and Protocols muestra la información sobre los puertos de los servicios que se instalan de forma predeterminada. Si instala otros VIB en el host, es posible que estén disponibles otros puertos de firewall y servicios adicionales. La información es principalmente para los servicios que están visibles en vSphere Client, pero la herramienta VMware Ports and Protocols también incluye otros puertos.

Comportamiento de firewall del cliente NFS

El conjunto de reglas de firewall del cliente NFS se comporta de forma diferente a otros conjuntos de reglas de firewall de ESXi. ESXi configura los parámetros del cliente NFS cuando se monta o desmonta una almacén de datos de NFS. El comportamiento varía según la versión de NFS.

Cuando se agrega, monta o desmonta un almacén de datos de NFS, el comportamiento que se obtiene varía según la versión de NFS.

Comportamiento de firewall de NFS v3

Cuando se agrega o monta un almacén de datos de NFS v3, ESXi comprueba el estado del conjunto de reglas de firewall del cliente NFS (`nfsClient`).

- Si el conjunto de reglas `nfsClient` está desactivado, ESXi activa el conjunto de reglas y desactiva la directiva Permitir todas las direcciones IP estableciendo la marca `allowedAll` en `FALSE`. La dirección IP del servidor NFS se agrega a la lista de direcciones IP salientes permitidas.
- Si el conjunto de reglas `nfsClient` está activado, el estado del conjunto de reglas y la directiva de direcciones IP permitidas no se cambian. La dirección IP del servidor NFS se agrega a la lista de direcciones IP salientes permitidas.

Nota Si activa manualmente el conjunto de reglas `nfsClient` o configura manualmente la directiva Permitir todas las direcciones IP, ya sea antes o después de agregar un almacén de datos de NFS v3 al sistema, la configuración se anula cuando se desmonta el último almacén de datos de NFS v3. El conjunto de reglas `nfsClient` se desactiva cuando se desmontan todos los almacenes de datos de NFS v3.

Cuando se quita o se desmonta un almacén de datos de NFS v3, ESXi realiza una de las siguientes acciones.

- Si ninguno de los almacenes de datos de NFS v3 restantes se monta desde el servidor del almacén de datos que se desmonta, ESXi quita la dirección IP del servidor de la lista de direcciones IP salientes.

- Si ninguno de los almacenes de datos de NFS v3 montados permanece después de la operación de desmontaje, ESXi desactiva el conjunto de reglas de firewall de `nfsClient`.

Comportamiento de firewall de NFS v4.1

Cuando se monta el primer almacén de datos de NFS v4.1, ESXi activa el conjunto de reglas `nfs41client` y establece su marca `allowedAll` en TRUE. Esta acción abre el puerto 2049 para todas las direcciones IP. Cuando se desmonta el almacén de datos NFS v4.1, el estado del firewall no se ve afectado. De esta forma, el primer montaje de NFS v4.1 abre el puerto 2049 y ese puerto permanece activado a menos que se cierre explícitamente.

Usar comandos de firewall ESXCLI para configurar el comportamiento de ESXi

Si el entorno incluye varios hosts ESXi, automatice la configuración del firewall usando comandos ESXCLI o vSphere Web Services SDK.

Referencia de comandos de firewall

Se pueden utilizar los comandos de ESXi Shell o ESXCLI en la línea de comandos para configurar ESXi para automatizar la configuración del firewall. Para manipular firewalls y reglas de firewall, consulte *Introducción a ESXCLI* para ver una introducción y *Conceptos y ejemplos de ESXCLI* para ver ejemplos de uso de ESXCLI.

En ESXi 7.0 y versiones posteriores, se restringe el acceso al archivo de `service.xml`, que se utiliza para crear reglas de firewall personalizadas. Consulte el artículo 2008226 de la base de conocimientos de VMware para obtener información sobre cómo crear reglas de firewall personalizadas usando el archivo `/etc/rc.local.d/local.sh`.

Tabla 3-6. Comandos de firewall

Comando	Descripción
`esxcli network firewall get`	Devuelva el estado del firewall y enumere las acciones predeterminadas.
`esxcli network firewall set --default-action`	Se establece en true para definir que la acción predeterminada sea pasar. Se establece en false para definir que la acción predeterminada sea anular.
`esxcli network firewall set --enabled`	Active o desactive el firewall ESXi.
`esxcli network firewall load`	Carga los archivos de configuración del conjunto de módulos y reglas del firewall.
`esxcli network firewall refresh`	Actualiza la configuración del firewall mediante la lectura de los archivos del conjunto de reglas si se carga el módulo de firewall.
`esxcli network firewall unload`	Destruye los filtros y descarga el módulo de firewall.
`esxcli network firewall ruleset list`	Enumera la información de los conjuntos de reglas.
`esxcli network firewall ruleset set --allowed-all`	Se establece en true para permitir un acceso total a todas las direcciones IP, o en false para utilizar una lista de direcciones IP permitidas.

Tabla 3-6. Comandos de firewall (continuación)

Comando	Descripción
`esxcli network firewall ruleset set --enabled --ruleset-id=<string>`	Se establece en true para activar el conjunto de reglas especificado. Se establece en false para desactivar el conjunto de reglas especificado.
`esxcli network firewall ruleset allowedip list`	Enumera las direcciones IP permitidas del conjunto de reglas especificado.
`esxcli network firewall ruleset allowedip add`	Permite acceder al conjunto de reglas desde la dirección IP o el intervalo de direcciones IP especificado.
`esxcli network firewall ruleset allowedip remove`	Quita el acceso al conjunto de reglas desde la dirección IP o el intervalo de direcciones IP especificados.
`esxcli network firewall ruleset rule list`	Enumera las reglas de cada conjunto de reglas del firewall.

Activar o desactivar un servicio de ESXi

Puede activar o desactivar servicios de ESXi desde vSphere Client.

Un host ESXi incluye varios servicios que se ejecutan de manera predeterminada. Si la directiva de la empresa lo permite, puede desactivar servicios desde el perfil de seguridad o activarlos.

Nota La activación de servicios afecta a la seguridad del host. No active un servicio a menos que sea estrictamente necesario.

Después de la instalación, algunos servicios se ejecutan de manera predeterminada, pero otros se interrumpen. En ocasiones, debe realizar otros pasos antes de que un servicio esté disponible en la interfaz de usuario. Por ejemplo, el servicio NTP es una forma de obtener información de tiempo precisa, pero este servicio solamente funciona cuando se abren los puertos requeridos en el firewall.

Los servicios disponibles dependen de los VIB que están instalados en el host ESXi. No puede agregar servicios sin instalar un VIB. Algunos productos de VMware, por ejemplo vSphere HA, instalan los VIB en los hosts para que los servicios y sus correspondientes puertos de firewall estén disponibles.

En una instalación predeterminada, puede modificar el estado de los siguientes servicios desde vSphere Client.

Tabla 3-7. Servicios de ESXi en el perfil de seguridad

Servicio	Predeterminado	Descripción
Interfaz de usuario de consola directa	En ejecución	El servicio de la interfaz de usuario de la consola directa (DCUI) permite interactuar con un host ESXi desde el host de la consola local mediante menús basados en texto.
ESXi Shell	Detenido	ESXi Shell está disponible desde la DCUI e incluye un conjunto de comandos totalmente compatibles, así como un conjunto de comandos para solucionar problemas y corregir errores. Debe activar el acceso a ESXi Shell desde la consola directa de cada sistema. Puede activar el acceso a la instancia de ESXi Shell local o el acceso a ESXi Shell mediante SSH.
SSH	Detenido	El servicio de cliente SSH en el host que permite las conexiones remotas a través de Secure Shell.
attestd	Detenido	Servicio de atestación de vSphere Trust Authority.
dpd	Detenido	Daemon de protección de datos.
Daemon para la formación de equipos basada en cargas	En ejecución	Formación de equipos basada en cargas.
kmxd	Detenido	Servicio de proveedor de claves de vSphere Trust Authority.
Servicio de Active Directory	Detenido	Este servicio se inicia al configurar ESXi para Active Directory.
Daemon de NTP	Detenido	Daemon del protocolo Network Time Protocol.
Daemon de tarjeta inteligente PC/SC	Detenido	Este servicio se inicia cuando se activa el host para la autenticación de tarjeta inteligente. Consulte Configurar y administrar la autenticación de tarjeta inteligente para ESXi.
Servidor CIM	En ejecución	Servicio que las aplicaciones del modelo de información común pueden utilizar (CIM).
slpd	Detenido	Daemon del protocolo de ubicación del servicio.
Servidor SNMP	Detenido	Daemon del SNMP. Consulte la documentación de *Supervisión y rendimiento de vSphere* para obtener información sobre cómo configurar el SNMP v1, v2 y v3.
Servicio VTDC	En ejecución	Servicio recopilador de seguimiento distribuido de vSphere.
vltd	Detenido	Daemon de transporte de LWD de VCDR.
Servidor de Syslog	Detenido	Daemon de Syslog. Puede activar Syslog desde la configuración avanzada del sistema en vSphere Client. Consulte la documentación de *Instalar y configurar vCenter Server*.

Tabla 3-7. Servicios de ESXi en el perfil de seguridad (continuación)

Servicio	Predeterminado	Descripción
VMware vCenter Agent	En ejecución	Agente de vCenter Server. Permite que vCenter Server se conecte a un host ESXi. Específicamente, vpxa es el canal de comunicación con el daemon del host que, a su vez, se comunica con el kernel de ESXi.
Servidor X.Org	Detenido	Servidor X.Org. Esta característica opcional es de uso interno para los gráficos 3D de las máquinas virtuales.

Requisitos previos

Conéctese a vCenter Server con vSphere Client.

Procedimiento

1 Desplácese hasta un host ESXi del inventario.

2 En **Sistema**, haga clic en **Configurar** y, a continuación, en **Servicios**.

3 Seleccione el servicio que desee cambiar.

   a Seleccione **Reiniciar**, **Iniciar** o **Detener** para hacer un cambio por única vez en el estado del host.

   b Para cambiar el estado del host en todos los reinicios, haga clic en **Editar directiva de inicio** y seleccione una directiva.

   - **Iniciar y detener con host**: el servicio se inicia poco después de que se enciende el host, y se cierra poco después de que se apaga el host. Al igual que **Iniciar y detener con uso de puerto**, esta opción implica que el servicio intenta regularmente completar sus tareas, como ponerse en contacto con el servidor NTP especificado. Si el puerto se cerró, pero luego se abre, el cliente empieza a completar las tareas poco tiempo después.
   - **Iniciar y detener manualmente**: el host conserva la configuración del servicio determinada por el usuario, más allá de que los puertos estén abiertos o cerrados. Cuando un usuario inicia el servicio NTP, el servicio sigue en ejecución si se enciende el host. Si el servicio se inicia y el host está desconectado, el servicio se detiene como parte del proceso de apagado. Cuando el host está encendido, el servicio se vuelve a iniciar, lo que conserva el estado determinado por el usuario.
   - **Iniciar y detener con uso de puerto**: el ajuste predeterminado para estos servicios. Si existe algún puerto abierto, el cliente intenta comunicarse con los recursos de red del servicio. Si existen algunos puertos abiertos, pero el puerto de un servicio específico está cerrado, se produce un error en el intento. Si el puerto saliente correspondiente está abierto, el servicio comienza a completar el inicio.

   Nota Esta configuración se aplica únicamente a la configuración de servicio establecida mediante la interfaz de usuario o a las aplicaciones creadas en vSphere Web Services SDK. Toda configuración establecida por otros medios, como desde ESXi Shell o mediante archivos de configuración, no se ve afectada por esta configuración.

4 Haga clic en **Aceptar**.

Configurar y administrar el modo de bloqueo en hosts ESXi

Para mejorar la seguridad de los hosts ESXi, puede ponerlos en modo de bloqueo. En el modo de bloqueo, las operaciones deben realizarse mediante vCenter Server de forma predeterminada.

Puede seleccionar entre el modo de bloqueo normal o el estricto, que ofrecen diferentes grados de bloqueo. También puede utilizar la lista de usuarios con excepción. Los usuarios con excepción no pierden sus privilegios cuando el host entra en el modo de bloqueo. Utilice la lista de usuarios con excepción para agregar cuentas de soluciones de terceros y aplicaciones externas que deben tener acceso directo al host cuando este último está en modo de bloqueo.

Comportamiento del modo de bloqueo

En el modo de bloqueo, algunos dispositivos se desactivan y algunos servicios quedan accesibles solo para ciertos usuarios.

Servicios de modo de bloqueo disponibles para diferentes usuarios

Cuando el host está en ejecución, los servicios disponibles dependen de si el modo de bloqueo está activado y del tipo de modo de bloqueo.

- En modo de bloqueo estricto y normal, los usuarios con privilegios pueden acceder al host mediante vCenter Server, desde vSphere Client o mediante el uso de vSphere Web Services SDK.
- El comportamiento de la interfaz de la consola directa no es igual en el modo de bloqueo estricto que en el modo de bloqueo normal.
  - En el modo de bloqueo estricto, el servicio de interfaz de usuario de la consola directa (DCUI) está desactivado.
  - En el modo de bloqueo normal, las cuentas de la lista de usuarios con excepción pueden acceder a la DCUI si poseen privilegios de administrador. Además, todos los usuarios que se especifican en la opción avanzada del sistema `DCUI.Access` pueden acceder a la DCUI.
- Si ESXi Shell o SSH están activados y el host se encuentra en el modo de bloqueo, las cuentas de la lista de usuarios con excepción que tienen privilegios de administrador pueden usar estos servicios. Para los demás usuarios, el acceso a ESXi Shell o SSH queda desactivado. Se cierran las sesiones de ESXi o SSH de usuarios que no tienen privilegios de administrador.

Todas las operaciones de acceso se registran para ambos modos de bloqueo, estricto y normal.

Tabla 3-8. Comportamiento del modo de bloqueo

Servicio	Modo normal	Modo de bloqueo normal	Modo de bloqueo estricto
vSphere Web Services API	Todos los usuarios, según los permisos	vCenter (vpxuser) Usuarios con excepción, según los permisos vCloud Director (vslauser, si está disponible)	vCenter (vpxuser) Usuarios con excepción, según los permisos vCloud Director (vslauser, si está disponible)
Proveedores de CIM	Usuarios con privilegios de administrador en el host	Usuarios con excepción de vCenter (vpxuser), según los permisos vCloud Director (vslauser, si está disponible)	Usuarios con excepción de vCenter (vpxuser), según los permisos vCloud Director (vslauser, si está disponible)
UI de consola directa (DCUI)	Usuarios con privilegios de administrador en el host y usuarios que se encuentran en la configuración avanzada del sistema `DCUI.Access`	Usuarios definidos en la configuración avanzada del sistema `DCUI.Access` Usuarios con excepción con privilegios de administrador en el host	El servicio de DCUI se detiene.
ESXi Shell (si está activado) y SSH (si está activado)	Usuarios con privilegios de administrador en el host	Usuarios definidos en la opción avanzada `DCUI.Access` Usuarios con excepción con privilegios de administrador en el host	Usuarios definidos en la configuración avanzada del sistema `DCUI.Access` Usuarios con excepción con privilegios de administrador en el host

Comportamiento del modo de bloqueo para los usuarios que inician sesión en ESXi Shell cuando el modo de bloqueo está activado

Los usuarios pueden iniciar sesión en ESXi Shell o acceder al host a través de SSH antes de activar el modo de bloqueo. En ese caso, la sesión de los usuarios que estén en la lista de usuarios con excepción y que tengan privilegios de administrador en el host permanecerá activa. La sesión se cierra para los demás usuarios. La finalización se aplica tanto al modo de bloqueo normal como al estricto.

Cómo puede desactivar el modo de bloqueo

El modo de bloqueo se puede desactivar de la siguiente manera.

Desde vSphere Client

Los usuarios pueden desactivar el modo de bloqueo normal y el modo de bloqueo estricto desde vSphere Client. Consulte Desactivar el modo de bloqueo desde vSphere Client.

Desde la interfaz de usuario de la consola directa

Los usuarios que pueden acceder a la interfaz de usuario de la consola directa en el host ESXi pueden desactivar el modo de bloqueo normal. En el modo de bloqueo estricto, el servicio de interfaz de la consola directa se detiene. Consulte Activar o desactivar el modo de bloqueo normal desde la interfaz de usuario de la consola directa.

Activar el modo de bloqueo desde vSphere Client

Seleccione el modo de bloqueo para requerir que todos los cambios en la configuración del host pasen por vCenter Server. vSphere admite el modo de bloqueo normal y el modo de bloqueo estricto.

Si prefiere no permitir todo acceso directo a un host por completo, puede seleccionar el modo de bloqueo estricto. El modo de bloqueo estricto impide que se acceda a un host si vCenter Server no está disponible y SSH y ESXi Shell están desactivados. Consulte Comportamiento del modo de bloqueo.

Procedimiento

1 Desplácese hasta el host en el inventario de vSphere Client.

2 Haga clic en **Configurar**.

3 En Sistema, seleccione **Perfil de seguridad**.

4 En el panel Modo de bloqueo, haga clic en **Editar**.

5 Haga clic en **Modo de bloqueo** y seleccione una de las opciones del modo de bloqueo.

Opción	Descripción
Normal	Se puede acceder al host desde vCenter Server. Solo los usuarios que están en la lista de usuarios con excepción y tienen privilegios de administrador pueden iniciar sesión en la interfaz de usuario de la consola directa. Si SSH o ESXi Shell están activados, es posible que se pueda tener acceso.
Estricto	Se puede acceder al host únicamente desde vCenter Server. Si se activan SSH o ESXi Shell, se mantienen habilitadas las sesiones en ejecución en las cuentas con el ajuste avanzado `DCUI.Access` y las cuentas de usuarios con excepción que tienen privilegios de administrador. Todas las demás sesiones se cierran.

6 Haga clic en **Aceptar**.

Desactivar el modo de bloqueo desde vSphere Client

Desactive el modo de bloqueo para permitir cambios de configuración en las conexiones directas al host ESXi. Si el modo de bloqueo está activado, el entorno es más seguro.

Los usuarios pueden desactivar el modo de bloqueo normal y el modo de bloqueo estricto desde vSphere Client.

Procedimiento

1 Desplácese hasta un host en el inventario de vSphere Client.

2 Haga clic en **Configurar**.

3 En Sistema, seleccione **Perfil de seguridad**.

4 En el panel Modo de bloqueo, haga clic en **Editar**.

5 Haga clic en **Modo de bloqueo** y seleccione **Deshabilitado** para desactivar el modo de bloqueo.

6 Haga clic en **Aceptar**.

Resultados

El sistema sale del modo de bloqueo, vCenter Server muestra una alarma y se agrega una entrada al registro de auditoría.

Activar o desactivar el modo de bloqueo normal desde la interfaz de usuario de la consola directa

Puede activar y desactivar el modo de bloqueo normal desde la interfaz de usuario de la consola directa (DCUI). El modo de bloqueo estricto puede activarse y desactivarse únicamente desde vSphere Client.

Cuando el host se encuentra en el modo normal de bloqueo, las siguientes cuentas pueden acceder a la interfaz de usuario de la consola directa:

- Cuentas en la lista de usuarios con excepción que tienen privilegios de administrador en el host. La lista de usuarios con excepción sirve para cuentas de servicios, como un agente de copia de seguridad.
- Usuarios definidos en la opción avanzada `DCUI.Access` del host. Esta opción puede utilizarse para activar el acceso en caso de que ocurra un error grave.

Los permisos de usuario se conservan cuando se activa el modo de bloqueo. Los permisos de usuario se restauran al desactivar el modo de bloqueo desde la interfaz de la consola directa.

Nota Si actualiza un host que se encuentra en el modo de bloqueo a la versión 6.0 de ESXi sin salir de ese modo, y si sale del modo después de actualizar, se perderán todos los permisos definidos antes de que el host entrara en el modo de bloqueo. El sistema asigna la función de administrador a todos los usuarios que se encuentran en la opción avanzada `DCUI.Access` para garantizar el acceso al host.

Para conservar los permisos, desactive el modo de bloqueo del host desde vSphere Client antes de realizar la actualización.

Procedimiento

1 En la interfaz de usuario de la consola directa del host, presione F2 e inicie sesión.

2 Desplácese hasta la opción **Configurar el modo de bloqueo** y presione Entrar para alternar la configuración actual.

3 Presione Esc hasta que vuelva al menú principal de la interfaz de usuario de la consola directa.

Especificar cuentas con privilegios de acceso en el modo de bloqueo

Puede especificar cuentas de servicio que puedan acceder al host ESXi. Para ello, agréguelas directamente a la lista de usuarios con excepción. Puede especificar que un único usuario acceda al host ESXi en caso de que se produzca un error grave en vCenter Server.

Qué pueden hacer las cuentas cuando vSphere está en modo de bloqueo

La versión de vSphere determina qué pueden hacer diferentes cuentas de forma predeterminada cuando se activa el modo de bloqueo y cómo se puede cambiar el comportamiento predeterminado.

- En vSphere 5.0 y versiones anteriores, únicamente el usuario raíz puede iniciar sesión en la interfaz de usuario de la consola directa (DCUI) en un host ESXi que se encuentra en el modo de bloqueo.
- En vSphere 5.1 y las versiones posteriores, puede agregar un usuario a la configuración avanzada del sistema `DCUI.Access` para cada host. El ajuste está pensado para un error grave de vCenter Server. Por lo general, las empresas bloquean la contraseña del usuario con este acceso en un lugar seguro. Un usuario de la lista `DCUI.Access` no necesita tener privilegios administrativos completos en el host.
- En vSphere 6.0 y las versiones posteriores, la configuración avanzada del sistema `DCUI.Access` sigue siendo compatible. Asimismo, vSphere 6.0 y las versiones posteriores admiten una lista de usuarios con excepción, destinada a las cuentas de servicio que deben conectarse al host directamente. Las cuentas con privilegios de administrador que figuran en la lista de usuarios con excepción pueden iniciar sesión en ESXi Shell. Por otra parte, estos usuarios pueden iniciar sesión en la DCUI de un host en el modo de bloqueo normal y pueden salir del modo de bloqueo.

  Especifique los usuarios con excepción desde vSphere Client.

  Nota Los usuarios con excepción son usuarios locales del host o usuarios de Active Directory con privilegios definidos localmente para el host ESXi. Los usuarios que son miembros de un grupo de Active Directory pierden sus permisos cuando el host se coloca en modo de bloqueo.

Agregar usuarios a la configuración avanzada del sistema DCUI.Access

Si se produce un error grave, la configuración avanzada del sistema `DCUI.Access` permite salir del modo de bloqueo cuando no se puede acceder al host desde vCenter Server. Para agregar usuarios a la lista, edite las opciones de configuración avanzada del host desde vSphere Client.

Nota Los usuarios de la lista de DCUI.Access pueden cambiar la configuración del modo de bloqueo independientemente de los privilegios que tengan. La capacidad de cambiar los modos de bloqueo puede afectar a la seguridad del host. En el caso de las cuentas de servicio que necesitan acceso directo al host, puede ser conveniente agregar usuarios a la lista de usuarios con excepción. Los usuarios con excepción solamente pueden realizar las tareas para las cuales tienen privilegios. Consulte "Especificar usuarios con excepción para el modo de bloqueo" más adelante en este tema.

---

1 Desplácese hasta el host en el inventario de vSphere Client.
2 Haga clic en **Configurar**.
3 En Sistema, haga clic en **Configuración avanzada del sistema** y en **Editar**.
4 Filtre por DCUI.
5 En el cuadro de texto **DCUI.Access**, introduzca los nombres de usuarios locales de ESXi separados por comas.

   Nota No puede introducir usuarios de Active Directory. Solo se admiten usuarios de ESXi locales.

   Se incluye al usuario raíz de forma predeterminada. Considere quitar al usuario raíz de la lista de DCUI.Access y especificar una cuenta con nombre para mejorar el proceso de auditoría.
6 Haga clic en **Aceptar**.

Especificar usuarios con excepción para el modo de bloqueo

Puede agregar usuarios a la lista de usuarios con excepción desde vSphere Client. Estos usuarios no pierden sus permisos cuando el host entra en el modo de bloqueo.

Es frecuente que esos usuarios tengan cuentas que representen soluciones y aplicaciones externas que necesitan seguir funcionando en el modo de bloqueo. Por ejemplo, es lógico agregar cuentas de servicio, como un agente de copia de seguridad, a la lista de usuarios con excepción.

Nota La lista de usuarios con excepción no está pensada para administradores sino para las cuentas de servicio que realizan tareas muy específicas. Agregar usuarios administradores a la lista de usuarios con excepción va en contra de la finalidad del modo de bloqueo.

Los usuarios con excepción son usuarios locales del host o usuarios de Active Directory con privilegios definidos localmente para el host ESXi. No son miembros de un grupo de Active Directory y no son usuarios de vCenter Server. Estos usuarios tienen permitido realizar operaciones en el host en función de sus privilegios. Esto significa, por ejemplo, que un usuario de solo lectura no puede desactivar el modo de bloqueo en un host.

1 Desplácese hasta el host en el inventario de vSphere Client.

2 Haga clic en **Configurar**.

3 En Sistema, seleccione **Perfil de seguridad**.

4 En el panel Modo de bloqueo, haga clic en **Editar**.

5 Haga clic en **Usuarios con excepción** y en el icono **Agregar usuario** para agregar usuarios con excepción.

6 Haga clic en **Aceptar**.

Usar paquetes de instalación de vSphere para realizar actualizaciones seguras

Para actualizar ESXi con ESXCLI, es necesario conocer bien los paquetes de instalación de vSphere, los perfiles de imagen y los almacenes de software.

ESXi consiste en un perfil de imagen, que describe un conjunto de paquetes de instalación (Installation Dundles, VIB) de vSphere que contienen el software real. Un VIB es un disco RAM firmado que representa un componente del sistema, aproximadamente análogo a un RPM o DEB en un sistema Linux. Un perfil de imágenes es una colección de VIB. Un almacén de software es una colección de VIB y perfiles de imagen. ESXi revisiones y almacenes contienen perfiles de imagen actualizados compuestos por un conjunto común de VIB.

Puede instalar actualizaciones ESXi en un host independiente mediante los comandos `esxcli software`. Para obtener más información, consulte la documentación sobre *Actualizar VMware ESXi*.

Nota Por lo general, en un entorno vSphere 7.0 y versiones posteriores, se utiliza VMware vSphere® vSphere Lifecycle Manager para administrar el ciclo de vida de los hosts ESXi.

Para enumerar todos los VIB instalados y su versión actual, o el perfil de imagen actual, puede utilizar los siguientes comandos ESXCLI.

- `esxcli software vib list`
- `esxcli software profile get`

En general, los pasos de alto nivel para actualizar ESXi de forma segura son los siguientes:

- Poner el host ESXi en modo de mantenimiento.
- Ejecutar un comando `esxcli software profile update`, que apunta a una URL o un archivo ZIP transferido al host a través de SSH

- Reiniciar el host ESXi

Debido a que VMware firma los VIB de forma criptográfica, no es necesaria la transferencia segura de los VIB o de todo el almacén, y el proceso de actualización verifica estas firmas.

Administrar los niveles de aceptación de los hosts ESXi y los paquetes de instalación de vSphere

El nivel de aceptación de un paquete de instalación de vSphere (VIB, vSphere Installation Bundle) depende de la cantidad de certificaciones de ese VIB. El nivel de aceptación del host ESXi depende del nivel del VIB más bajo. Si desea permitir VIB de menor nivel, puede cambiar el nivel de aceptación del host. Puede eliminar los VIB CommunitySupported para tener la posibilidad de cambiar el nivel de aceptación del host.

Los VIB son paquetes de software que incluyen una firma de VMware o un partner de VMware. Para conservar la integridad del host ESXi, no permita que los usuarios instalen VIB no firmados (creados por la comunidad). Un VIB no firmado contiene un código no certificado, aceptado ni admitido por VMware o sus partners. Los VIB creados por la comunidad no tienen una firma digital.

El nivel de aceptación del host ESXi debe ser igual de restrictivo o menos restrictivo que el nivel de aceptación de cualquier VIB que se desee agregar al host. Por ejemplo, si el nivel de aceptación del host es VMwareAccepted, no se puede instalar VIB en el nivel PartnerSupported. Es posible utilizar los comandos ESXCLI para establecer un nivel de aceptación de un host. Para proteger la seguridad y la integridad de los hosts ESXi, no permita que se instalen VIB no firmados (CommunitySupported) en los hosts de sistemas de producción.

El nivel de aceptación para un host ESXi se muestra en **Perfil de seguridad**, en vSphere Client.

Los siguientes niveles de aceptación son compatibles.

VMwareCertified

El nivel de aceptación VMwareCertified tiene los requisitos más estrictos. Los VIB con este nivel se someten a pruebas completamente equivalentes a las pruebas de control de calidad internas de VMware para la misma tecnología. Hoy en día, solo los controladores de los programas de proveedores de E/S (I/O Vendor Program, IOVP) se publican en este nivel. VMware responde a las llamadas de soporte para VIB con este nivel de aceptación.

VMwareAccepted

Los VIB con este nivel de aceptación pasan por pruebas de comprobación, pero estas no prueban completamente todas las funciones del software. El partner realiza pruebas y VMware comprueba el resultado. Hoy en día, los proveedores de CIM y los complementos de PSA son algunos de los VIB que se publican en este nivel. VMware indica a los clientes que realizan llamadas de soporte para VIB con este nivel de aceptación que se pongan en contacto con la organización de soporte del partner.

PartnerSupported

Los VIB con el nivel de aceptación PartnerSupported los publica un partner de confianza de VMware. El partner realiza todas las pruebas. VMware no comprueba los resultados. Este nivel se utiliza para una tecnología nueva o alternativa que los partners desean habilitar para los sistemas VMware. Hoy en día, las tecnologías de VIB de controlador, como Infiniband, ATAoE y SSD, se encuentran en este nivel con controladores de hardware que no son estándar. VMware indica a los clientes que realizan llamadas de soporte para VIB con este nivel de aceptación que se pongan en contacto con la organización de soporte del partner.

CommunitySupported

El nivel de aceptación CommunitySupported es para VIB creados por personas o empresas por fuera de los programas de partners de VMware. Los VIB de este nivel de aceptación no pasaron por un programa de pruebas aprobado por VMware y no son compatibles con el soporte técnico de VMware ni los partners de VMware.

Procedimiento

1. Conéctese a cada host ESXi mediante SSH.
2. Compruebe que el nivel de aceptación esté establecido en VMwareCertified, VMwareAccepted o PartnerSupported con el siguiente comando.

```
esxcli software acceptance get
```

3. Si el nivel de aceptación del host es CommunitySupported, determine si cualquiera de los VIB están en el nivel CommunitySupported con uno de los siguientes comandos.

```
esxcli software vib list
esxcli software vib get -n vibname
```

4. Elimine todos los VIB CommunitySupported con el siguiente comando.

```
esxcli software vib remove --vibname vib
```

5. Cambie el nivel de aceptación del host mediante uno de los siguientes métodos.

Opción	Descripción
Comando de la CLI	`esxcli software acceptance set --level level` El parámetro `level` es obligatorio y especifica el nivel de aceptación que se va a establecer. Debe ser **`VMwareCertified`**, **`VMwareAccepted`**, **`PartnerSupported`** o **`CommunitySupported`**. Consulte *Referencia de ESXCLI* para obtener más información.
vSphere Client	a Seleccione un host en el inventario. b Haga clic en **Configurar**. c En Sistema, seleccione **Perfil de seguridad**. d Haga clic en **Editar** de Nivel de aceptación del perfil de imagen del host y seleccione el nivel de aceptación.

Resultados

El nuevo nivel de aceptación está en vigor.

Nota ESXi realiza comprobaciones de integridad de los VIB regido por el nivel de aceptación. Puede usar la configuración de `VMkernel.Boot.execInstalledOnly` para indicar a ESXi que solo ejecuten archivos binarios que se originen de un VIB válido instalado en el host. Junto con el arranque seguro, esta configuración garantiza que todos los procesos que se ejecuten en ESXi host están firmados, permitidos y esperados. De forma predeterminada, el ajuste `VMkernel.Boot.execInstalledOnly` está desactivado para la compatibilidad de socios en vSphere 7.0 y versiones posteriores. Si esta opción se activa cuando sea posible, mejorará la seguridad. Para obtener más información sobre la configuración de opciones avanzadas para ESXi, consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/1038578.

Asignar privilegios para hosts ESXi

Normalmente, se otorgan privilegios a los usuarios mediante la asignación de permisos para los objetos de los hosts ESXi que administra un sistema vCenter Server. Si se utiliza un host ESXi independiente, se pueden asignar los privilegios directamente.

Asignar permisos para hosts ESXi administrados por vCenter Server

Si el host ESXi está administrado por vCenter Server, realice las tareas de administración a través de vSphere Client.

Puede seleccionar el objeto de host ESXi en la jerarquía de objetos de vCenter Server y asignar la función de administrador a una cantidad limitada de usuarios. Esos usuarios podrán realizar entonces una administración directa en el host ESXi. Consulte Usar funciones de vCenter Server para asignar privilegios.

La práctica recomendada implica crear al menos una cuenta de usuario designado, asignarle privilegios administrativos completos en el host y utilizar esta cuenta en lugar de la cuenta raíz. Establezca una contraseña de alta complejidad para la cuenta raíz y limite la utilización de la cuenta raíz. No elimine la cuenta raíz.

Asignar permisos para hosts independientes de ESXi

Se pueden agregar usuarios locales y definir funciones personalizadas desde la pestaña Administración de VMware Host Client. Consulte la documentación de *Administrar un host único de vSphere: VMware Host Client*.

Para todas las versiones de ESXi, puede ver la lista de usuarios predefinidos en el archivo `/etc/passwd`.

Las siguientes funciones están predefinidas.

Solo lectura

Permite que un usuario vea los objetos asociados con el host ESXi, pero no le permite realizar cambios en los objetos.

Administrador

Función de administrador.

Sin acceso

Sin acceso. Esta función es la función predeterminada. Es posible anular la función predeterminada.

Se pueden administrar grupos y usuarios locales, y agregar funciones locales personalizadas a un host ESXi mediante una instancia de VMware Host Client conectada directamente al host ESXi. Consulte la documentación de *Administrar un host único de vSphere: VMware Host Client*.

En vSphere 6.0 y versiones posteriores, es posible utilizar los comandos ESXCLI para la administración de cuentas de usuarios locales de ESXi. Los comandos ESXCLI de administración de permisos se pueden utilizar para configurar o quitar permisos tanto en cuentas de Active Directory (usuarios y grupos) como en cuentas locales de ESXi (usuarios únicamente).

Nota Si se define un usuario para el host ESXi mediante una conexión directa al host, y existe un usuario con el mismo nombre en vCenter Server, los usuarios son diferentes. Si se asigna una función al usuario de ESXi, al usuario de vCenter Server no se le asigna la misma función.

Privilegios y usuarios de ESXi predefinidos

Si el entorno no incluye un sistema vCenter Server, están predefinidos los siguientes usuarios.

Usuario raíz

Cada host ESXi tiene, de manera predeterminada, una sola cuenta de usuario raíz con la función de administrador. Esa cuenta de usuario raíz puede utilizarse para la administración local y para conectar el host a vCenter Server.

La asignación de privilegios de usuario raíz puede facilitar el ingreso a un host ESXi debido a que el nombre ya se conoce. Tener una cuenta raíz común también dificulta hacer coincidir acciones con usuarios.

Para optimizar la auditoría, cree cuentas individuales con privilegios de administrador. Establezca una contraseña de complejidad alta para la cuenta raíz y limite el uso de la cuenta, por ejemplo, para utilizar en el momento de agregar un host a vCenter Server. No elimine la cuenta raíz. Para obtener más información sobre la asignación de permisos a un usuario para un host ESXi, consulte el documento *Administrar un host único de vSphere: VMware Host Client*.

La práctica recomendada es que todas las cuentas con la función de administrador en un host ESXi se asignen a un usuario específico que tenga una cuenta con nombre. Utilice las funcionalidades de ESXi Active Directory que permiten administrar las credenciales de Active Directory.

Importante Puede quitar los privilegios de acceso al usuario raíz. Sin embargo, primero deberá crear otro permiso a nivel de raíz con otro usuario asignado a la función de administrador.

Usuario vpxuser

vCenter Server utiliza los privilegios del usuario vpxuser cuando se administran actividades del host.

El administrador de vCenter Server puede realizar casi todas las mismas tareas en el host que el usuario raíz y, también, programar tareas, trabajar con plantillas, etc. Sin embargo, el administrador de vCenter Server no puede crear, eliminar o editar usuarios y grupos locales para los hosts de forma directa. Solo un usuario con privilegios de administrador puede realizar estas tareas directamente en un host.

No se puede administrar el usuario vpxuser mediante Active Directory.

Precaución No modifique el usuario vpxuser de ninguna manera. No cambie su contraseña. No cambie sus permisos. Si lo hace, podría experimentar problemas al trabajar con los hosts a través de vCenter Server.

Usuario dcui

El usuario dcui se ejecuta en hosts y actúa con derechos de administrador. El fin principal de este usuario es configurar los hosts para el modo de bloqueo desde la interfaz de usuario de la consola directa (DCUI).

Este usuario actúa como agente para la consola directa, y los usuarios interactivos no pueden modificarlo ni usarlo.

Desactivar el acceso al shell para usuarios no raíz de ESXi

En vSphere 8.0 y versiones posteriores, puede desactivar el acceso al shell para los usuarios de ESXi no raíz, como los usuarios predefinidos vpxuser y dcui. Al desactivar el acceso al shell, puede mejorar la seguridad aplicando una postura de "solo API" para estos usuarios.

Para desactivar el acceso al shell, puede utilizar el comando `esxcli system account set --id` *user* `--shell-access false`. La API correspondiente es `LocalAccountManager.updateUser`. También puede utilizar VMware Host Client para cambiar el indicador Activar acceso al shell de los usuarios locales de ESXi.

Nota Cuando se desactiva el acceso al shell para un usuario con acceso administrativo, a causa de que se le deniega el acceso al shell, ese usuario no puede conceder acceso al shell a otros usuarios ni cambiar las contraseñas de los usuarios que tienen acceso al shell. Otros permisos, como los perfiles de host, seguirán permitiendo que los usuarios, como vpxuser y dcui, cambien las contraseñas de otros usuarios.

Al realizar cambios de este tipo, compruebe que no interrumpen los flujos de trabajo de terceros existentes.

Usar Active Directory para administrar usuarios de ESXi

Se puede configurar ESXi para utilizar un servicio de directorio como Active Directory con el fin de administrar usuarios.

La creación de cuentas de usuarios locales en cada host presenta desafíos para la sincronización de los nombres y las contraseñas de las cuentas en varios hosts. Conecte los hosts ESXi a un dominio de Active Directory para que no sea necesario crear y mantener cuentas de usuarios locales. La utilización de Active Directory para autenticar usuarios simplifica la configuración del host ESXi y reduce el riesgo de que ocurran problemas de configuración que podrían permitir un acceso no autorizado.

Al utilizar Active Directory, los usuarios suministran sus credenciales de Active Directory y el nombre de dominio del servidor de Active Directory cuando se agrega un host a un dominio.

Configurar un host ESXi para utilizar Active Directory

Si desea administrar usuarios y grupos, puede configurar un host ESXi para el uso de un servicio de directorio como Active Directory.

Cuando agrega un host ESXi en Active Directory, el grupo DOMAIN **ESX Admins** recibe acceso administrativo completo al host si este existe. Si no desea que quede disponible el acceso administrativo completo, consulte el artículo 1025569 de la base de conocimientos de VMware para encontrar una solución alternativa.

Si se aprovisiona un host con Auto Deploy, las credenciales de Active Directory no pueden almacenarse en los hosts. Puede usar vSphere Authentication Proxy para unir el host a un dominio de Active Directory. Dado que existe una cadena de confianza entre vSphere Authentication Proxy y el host, Authentication Proxy puede unir el host al dominio de Active Directory. Consulte Usar vSphere Authentication Proxy.

Nota Al momento de definir la configuración de la cuenta de usuario en Active Directory, es posible definir un límite para los equipos en los que un usuario puede iniciar sesión por el nombre de equipo. De forma predeterminada, no se establecen restricciones similares en una cuenta de usuario. Si se establece dicho límite, las solicitudes de enlaces LDAP de la cuenta de usuario generan errores y muestran el mensaje `Error en el enlace LDAP`, incluso si la solicitud proviene de un equipo que figura en la lista. Para evitar este problema, agregue el nombre netBIOS en el servidor de Active Directory a la lista de equipos en los cuales se puede iniciar sesión con la cuenta de usuario.

Requisitos previos

- Compruebe que tenga un dominio de Active Directory. Consulte la documentación del servidor del directorio.
- Compruebe que el nombre de host ESXi esté completo con el nombre de dominio del bosque de Active Directory.

  nombre de dominio completo = *host_name.domain_name*

Procedimiento

1. Sincronice el tiempo entre ESXi y el sistema de servicio del directorio.

   Consulte Sincronización de los relojes de ESXi con un servidor horario de red o la base de conocimientos de VMware para obtener información sobre cómo sincronizar la hora de ESXi con una controladora de dominio de Microsoft.

2. Asegúrese de que los servidores DNS que configuró en el host puedan resolver los nombres de host en las controladoras de Active Directory.

   a. Desplácese hasta el host en el inventario de vSphere Client.
   b. Haga clic en **Configurar**.
   c. En Redes, haga clic en **Configuración de TCP/IP**.
   d. En Pila de TCP/IP: Predeterminada, haga clic en **DNS** y compruebe que el nombre de host y la información del servidor DNS del host sean correctos.

Pasos siguientes

Una el host a un dominio de servicio de directorio. Consulte Agregar un host ESXi a un dominio de servicio de directorio. En los hosts que se aprovisionan con Auto Deploy, configure vSphere Authentication Proxy. Consulte Usar vSphere Authentication Proxy. Puede configurar permisos para que los usuarios y los grupos del dominio de Active Directory puedan acceder a los componentes de vCenter Server. Para obtener información sobre cómo administrar permisos, consulte Agregar un permiso a un objeto de inventario .

Agregar un host ESXi a un dominio de servicio de directorio

Para que el host ESXi utilice un servicio de directorio, se debe conectar el host al dominio de servicio de directorio.

Es posible introducir el nombre de dominio con uno de los dos métodos siguientes:

- **`name.tld`** (por ejemplo, **`domain.com`**): la cuenta se crea en el contenedor predeterminado.
- **`name.tld/container/path`** (por ejemplo, **`domain.com/OU1/OU2)`**: la cuenta se crea en una unidad organizativa (OU) en particular.

Para utilizar el servicio vSphere Authentication Proxy, consulte Usar vSphere Authentication Proxy.

Procedimiento

1 Desplácese hasta un host en el inventario de vSphere Client.
2 Haga clic en **Configurar**.
3 En Sistema, seleccione **Servicios de autenticación**.
4 Haga clic en **Unir dominio**.
5 Introduzca un dominio.

   Utilice el formulario **`name.tld`** o **`name.tld/container/path`**.

6 Introduzca el nombre de usuario y la contraseña de un usuario de servicio de directorio que tenga permisos para unir el host al dominio y, a continuación, haga clic en **Aceptar**.
7 (opcional) Si desea utilizar un proxy de autenticación, introduzca la dirección IP del servidor proxy.
8 Haga clic en **Aceptar** para cerrar el cuadro de diálogo Configuración de servicios de directorio.

Pasos siguientes

Puede configurar permisos para que los usuarios y los grupos del dominio de Active Directory puedan acceder a los componentes de vCenter Server. Para obtener información sobre cómo administrar permisos, consulte Agregar un permiso a un objeto de inventario .

Ver la configuración del servicio de directorio para un host ESXi

Puede ver el tipo de servidor de directorio (si lo hubiera) que utiliza el host ESXi para autenticar usuarios y su respectiva configuración.

Procedimiento

1 Desplácese hasta el host en el inventario de vSphere Client.

2 Haga clic en **Configurar**.

3 En Sistema, seleccione **Servicios de autenticación**.

   En la página Servicios de autenticación se muestra el servicio del directorio y la configuración del dominio.

Pasos siguientes

Puede configurar permisos para que los usuarios y los grupos del dominio de Active Directory puedan acceder a los componentes de vCenter Server. Para obtener información sobre cómo administrar permisos, consulte Agregar un permiso a un objeto de inventario .

Usar vSphere Authentication Proxy

Se pueden agregar hosts ESXi a un dominio de Active Directory mediante vSphere Authentication Proxy en lugar de agregarlos explícitamente al dominio de Active Directory.

Solo tiene que configurar el host de manera que conozca el nombre de dominio del servidor de Active Directory y la dirección IP de vSphere Authentication Proxy. Cuando vSphere Authentication Proxy está habilitado, automáticamente agrega hosts que se aprovisionan con Auto Deploy al dominio de Active Directory. También puede usar vSphere Authentication Proxy con hosts que no se aprovisionan mediante Auto Deploy.

Consulte Puertos necesarios en vCenter Server para obtener información sobre los puertos TCP que emplea vSphere Authentication Proxy.

Auto Deploy

Si aprovisiona hosts con Auto Deploy, puede configurar un host de referencia que apunte a Authentication Proxy. A continuación, debe configurar una regla que aplique el perfil del host de referencia a cualquier host ESXi que esté aprovisionado con Auto Deploy. vSphere Authentication Proxy almacena las direcciones IP de todos los hosts que Auto Deploy aprovisiona mediante PXE en la lista de control de acceso. Cuando el host arranca, se pone en contacto con vSphere Authentication Proxy, el cual une esos hosts, que ya están en la lista de control de acceso, al dominio de Active Directory.

Incluso si usa vSphere Authentication Proxy en un entorno que utiliza certificados aprovisionados por VMCA o certificados de terceros, el proceso funciona sin problemas si sigue las instrucciones para usar certificados personalizados con Auto Deploy.

Consulte Convertir a Auto Deploy en una autoridad de certificación subordinada.

Otros hosts ESXi

Se pueden configurar otros hosts para que usen vSphere Authentication Proxy si desea permitir que el host se una al dominio sin usar credenciales de Active Directory. Es decir, no necesita transmitir credenciales de Active Directory al host ni guardar credenciales de Active Directory en el perfil de host.

En ese caso, debe agregar la dirección IP del host a la lista de control de acceso de vSphere Authentication Proxy para que este autorice el host según su dirección IP predeterminada. Puede habilitar la autenticación del cliente para que vSphere Authentication Proxy realice la verificación del certificado del host.

Nota IPv6 es compatible en vSphere. No se admite en vSphere with Tanzu.

Iniciar el servicio vSphere Authentication Proxy

El servicio vSphere Authentication Proxy se encuentra disponible en cada sistema de vCenter Server. De forma predeterminada, el servicio no se encuentra en ejecución. Si desea usar vSphere Authentication Proxy en el entorno, puede iniciar el servicio desde la interfaz de administración de vCenter Server o desde la línea de comandos.

El servicio de vSphere Authentication Proxy se enlaza a una dirección IPv4 para comunicarse con vCenter Server y no admite IPv6. La instancia de vCenter Server puede residir en un equipo host de un entorno de red de solo IPv4 o de modo mixto IPv4/IPv6. Sin embargo, cuando se especifica la dirección de vSphere Authentication Proxy, se debe especificar una dirección IPv4.

Requisitos previos

Compruebe que utiliza vCenter Server 6.5 o de una versión posterior. En las versiones anteriores de vSphere, vSphere Authentication Proxy se instala por separado. Consulte la documentación de la versión anterior del producto para obtener instrucciones.

Procedimiento

1 Inicie el servicio de VMware vSphere Authentication Proxy.

Opción	Descripción
Interfaz de administración de vCenter Server	a En un explorador web, vaya a la interfaz de administración de vCenter Server, https://*dirección-IP-o-FQDN-de-vCenter*:5480. b Inicie sesión como raíz. La contraseña raíz predeterminada es la que estableció al implementar vCenter Server. c Haga clic en **Servicios** y en el servicio **VMware vSphere Authentication Proxy**. d Haga clic en **Iniciar**. e (opcional) Una vez iniciado el servicio, haga clic en **Establecer tipo de inicio** y haga en **Automático** para que el inicio sea automático.
CLI	`service-control --start vmcam`

2 Confirme que el servicio se inició correctamente.

Resultados

A continuación, se podrá establecer el dominio de vSphere Authentication Proxy. Después de eso, vSphere Authentication Proxy controlará todos los hosts aprovisionados con Auto Deploy y el usuario podrá agregar hosts de forma explícita a vSphere Authentication Proxy.

Agregar un dominio a vSphere Authentication Proxy con vSphere Client

Puede agregar un dominio a vSphere Authentication Proxy desde vSphere Client.

Puede agregar un dominio en vSphere Authentication Proxy únicamente después de habilitar el proxy. Después de agregar el dominio, vSphere Authentication Proxy agrega todos los hosts que se aprovisionan con Auto Deploy en ese dominio. En los demás hosts, también puede utilizar vSphere Authentication Proxy si no desea otorgar privilegios de dominio para esos hosts.

Procedimiento

1 Conéctese a un sistema vCenter Server con vSphere Client.

2 Seleccione vCenter Server y haga clic en **Configurar**.

3 Haga clic en **Authentication Proxy** y en **Editar**.

4 Introduzca el nombre del dominio al que vSphere Authentication Proxy agregará los hosts y el nombre y contraseña de un usuario con privilegios de Active Directory para agregar hosts al dominio.

5 Haga clic en **Guardar**.

Agregar un dominio a vSphere Authentication Proxy con el comando camconfig

Puede agregar un dominio a vSphere Authentication con el comando `camconfig`.

Puede agregar un dominio en vSphere Authentication Proxy únicamente después de habilitar el proxy. Después de agregar el dominio, vSphere Authentication Proxy agrega todos los hosts que se aprovisionan con Auto Deploy en ese dominio. En los demás hosts, también puede utilizar vSphere Authentication Proxy si no desea otorgar privilegios de dominio para esos hosts.

Procedimiento

1 Inicie sesión en el sistema vCenter Server como usuario con privilegios de administrador.

2 Ejecute el comando para habilitar el acceso al shell de Bash.

```
shell
```

3 Vaya al directorio `/usr/lib/vmware-vmcam/bin/`, donde se encuentra el script **camconfig**.

4 Para agregar las credenciales de usuario y de dominio de Active Directory a la configuración de Authentication Proxy, ejecute el siguiente comando.

```
camconfig add-domain -d domain -u user
```

Se le solicita una contraseña.

vSphere Authentication Proxy almacena ese nombre de usuario y esa contraseña en la memoria caché. Puede eliminar y volver a crear el usuario según se requiera. Debe ser posible acceder al dominio a través de DNS, pero no es necesario que sea un origen de identidad de vCenter Single Sign-On.

vSphere Authentication Proxy usa el nombre de usuario especificado por *user* para crear las cuentas de los hosts ESXi en Active Directory. El usuario debe tener privilegios para crear cuentas en el dominio de Active Directory al que se desea añadir los hosts. Al momento de escribir esta información, el artículo 932455 de Microsoft Knowledge Base brinda información complementaria sobre los privilegios de creación de cuentas.

5 Si más adelante desea eliminar la información de dominio y usuario de vSphere Authentication Proxy, ejecute el siguiente comando.

```
camconfig remove-domain -d domain
```

Usar vSphere Authentication Proxy para agregar un host a un dominio

El servidor Auto Deploy agrega todos los hosts que aprovisiona a vSphere Authentication Proxy, que agrega esos hosts al dominio. Si desea utilizar vSphere Authentication Proxy para agregar otros hosts a un dominio, puede agregarlos a vSphere Authentication Proxy explícitamente. A continuación, el servidor vSphere Authentication Proxy agrega esos hosts al dominio. Como

resultado, ya no es necesario que las credenciales suministradas por el usuario sean transmitidas al sistema de vCenter Server.

Es posible introducir el nombre de dominio con uno de los dos métodos siguientes:

- **`name.tld`** (por ejemplo, **`domain.com`**): la cuenta se crea en el contenedor predeterminado.
- **`name.tld/container/path`** (por ejemplo, **`domain.com/OU1/OU2)`**: la cuenta se crea en una unidad organizativa (OU) en particular.

Requisitos previos

- Si el host ESXi está utilizando un certificado firmado por VMCA, compruebe que el host se haya agregado a vCenter Server. De lo contrario, el servicio de Authentication Proxy no puede confiar en el host ESXi.
- Si el host ESXi está utilizando un certificado firmado por una entidad de certificación raíz, compruebe que se haya agregado el certificado firmado por la CA raíz correspondiente al sistema de vCenter Server. Consulte Administrar certificados para hosts ESXi.

Procedimiento

1 Desplácese hasta el host en el inventario de vSphere Client.

2 Haga clic en **Configurar**.

3 En **Sistema**, seleccione **Servicios de autenticación**.

4 Haga clic en **Unir dominio**.

5 Introduzca un dominio.

   Utilice el formato **`name.tld`**, por ejemplo **`midominio.com`**, o **`name.tld/container/path`**, por ejemplo, **`midominio.com/organizational_unit1/organizational_unit2`**.

6 Seleccione **Utilizar servidor proxy**.

7 Introduzca la dirección IP del servidor Authentication Proxy, que siempre es la misma que la dirección IP del sistema de vCenter Server.

8 Haga clic en **Aceptar**.

Activar la autenticación de cliente para vSphere Authentication Proxy

De forma predeterminada, vSphere Authentication Proxy agrega todo host que posea una dirección IP incluida en su lista de control de acceso. Para aumentar la seguridad, es posible activar la autenticación de cliente. Si se activa la autenticación de cliente, vSphere Authentication Proxy también comprueba el certificado del host.

Requisitos previos

- Compruebe que el sistema vCenter Server confíe en el host. De forma predeterminada, cuando se agrega un host a vCenter Server, se asigna al host un certificado con la firma de una entidad de certificación raíz de confianza de vCenter Server. vSphere Authentication Proxy confía en la entidad de certificación raíz de confianza de vCenter Server.
- Si planea reemplazar los certificados de ESXi en el entorno, realice el reemplazo antes de activar vSphere Authentication Proxy. Los certificados en el host ESXi deben coincidir con los del registro del host.

Procedimiento

1 Inicie sesión en el sistema vCenter Server como usuario con privilegios de administrador.

2 Active el acceso al shell de Bash mediante el comando `shell`.

3 Vaya al directorio `/usr/lib/vmware-vmcam/bin/`, donde se encuentra el script **camconfig**.

4 Para activar la autenticación del cliente, ejecute el siguiente comando.

```
camconfig ssl-cliAuth -e
```

En adelante, vSphere Authentication Proxy comprobará el certificado de cada host que se agregue.

5 Si más adelante desea volver a desactivar la autenticación de cliente, ejecute el siguiente comando.

```
camconfig ssl-cliAuth -n
```

Importar el certificado de vSphere Authentication Proxy en el host ESXi

De manera predeterminada, los hosts ESXi requieren la comprobación explícita del certificado de vSphere Authentication Proxy. Si usa vSphere Auto Deploy, el servicio de Auto Deploy se ocupa de agregar el certificado a los hosts que aprovisiona. Para otros hosts, el certificado se debe agregar de forma explícita.

Requisitos previos

- Cargue el certificado de vSphere Authentication Proxy en un almacén de datos accesible para el host ESXi. Mediante una aplicación SFTP como WinSCP, puede descargar el certificado del host de vCenter Server en la siguiente ubicación.

  `/var/lib/vmware/vmcam/ssl/rui.crt`

- Compruebe que la configuración avanzada de `UserVars.ActiveDirectoryVerifyCAMCertificate` ESXi esté establecida en 1 (valor predeterminado).

Procedimiento

1. Seleccione el host ESXi y haga clic en **Configurar**.
2. En **Sistema**, seleccione **Servicios de autenticación**.
3. Haga clic en **Importar certificado**.
4. Introduzca la ruta de acceso al archivo de certificado siguiendo el formato `[`*`datastore`*`]/`*`path`*`/`*`certname`*`.crt`.
5. Introduzca la dirección IP del servidor de vSphere Authentication Proxy.
6. Haga clic en **Aceptar**.

Generar un nuevo certificado para vSphere Authentication Proxy

Puede generar un nuevo certificado que esté aprovisionado por VMware Certificate Authority (VMCA) o un nuevo certificado que incluya a VMCA como certificado subordinado.

Consulte Configurar vSphere Authentication Proxy para usar certificados personalizados si desea usar un certificado que esté firmado por una entidad de certificación externa o empresarial.

Requisitos previos

Debe tener privilegios de raíz o de administrador sobre el sistema en el que se ejecuta vSphere Authentication Proxy.

Procedimiento

1. Haga una copia de `certool.cfg`.

   ```
   cp /usr/lib/vmware-vmca/share/config/certool.cfg /var/lib/vmware/vmcam/ssl/vmcam.cfg
   ```

2. Edite la copia con alguna información de su organización, como en el ejemplo siguiente.

   ```
   Country = IE
   Name = vmcam
   Organization = VMware
   OrgUnit = vTSU
   State = Cork
   Locality = Cork
   Hostname = test-cam-1.test1.vmware.com
   ```

3. Genere la nueva clave privada en `/var/lib/vmware/vmcam/ssl/`.

   ```
   /usr/lib/vmware-vmca/bin/certool --genkey --privkey=/var/lib/vmware/vmcam/ssl/rui.key --
   pubkey=/tmp/vmcam.pub --server=localhost
   ```

   Para *localhost*, suministre el FQDN de vCenter Server.

4 Genere el nuevo certificado en `/var/lib/vmware/vmcam/ssl/` usando la clave y el archivo `vmcam.cfg` que creó en el paso 1 y el paso 2.

```
/usr/lib/vmware-vmca/bin/certool --server=localhost --gencert --privkey=/var/lib/
vmware/vmcam/ssl/rui.key --cert=/var/lib/vmware/vmcam/ssl/rui.crt --config=/var/lib/vmware/
vmcam/ssl/vmcam.cfg
```

Para *localhost*, suministre el FQDN de vCenter Server.

Configurar vSphere Authentication Proxy para usar certificados personalizados

El uso de certificados personalizados con vSphere Authentication Proxy consta de varios pasos. Primero, genere una CSR y envíela a la entidad de certificación para que la firme. A continuación, coloque el certificado firmado y el archivo de clave en una ubicación a la que vSphere Authentication Proxy pueda acceder.

De manera predeterminada, vSphere Authentication Proxy genera una CSR durante el primer arranque y pide a VMCA que firme esa CSR. vSphere Authentication Proxy se registra con vCenter Server y usa ese certificado. Puede usar certificados personalizados en el entorno si los agrega a vCenter Server.

Procedimiento

1 Genere una CSR para vSphere Authentication Proxy.

a Cree un archivo de configuración, `/var/lib/vmware/vmcam/ssl/vmcam.cfg`, como se muestra en el siguiente ejemplo.

```
[ req ]
distinguished_name = req_distinguished_name
encrypt_key = no
prompt = no
string_mask = nombstr
req_extensions = v3_req
[ v3_req ]
basicConstraints = CA:false
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName = DNS:vcenter1.example.com
[ req_distinguished_name ]
countryName = US
stateOrProvinceName = NY
localityName = New York
0.organizationName = Example Inc.
organizationalUnitName = IT Org
commonName = vcenter1.example.com
```

Tenga en cuenta lo siguiente:

- subjectAltName: use el formato **DNS:***FQDN_of_vCenter_Appliance_to_use_the_CA-signed certificate*.
- commonName: utilice el mismo FQDN del dispositivo de vCenter utilizado en subjectAltName.

b Ejecute `openssl` para generar un archivo CSR y un archivo de claves, pasando el archivo de configuración.

```
openssl req -new -nodes -out vmcam.csr -newkey rsa:2048 -keyout /var/lib/vmware/
vmcam/ssl/rui.key -config /var/lib/vmware/vmcam/ssl/vmcam.cfg
```

2 Realice una copia de seguridad del certificado `rui.crt` y de los archivos `rui.key`, que están almacenados en la siguiente ubicación.

`/var/lib/vmware/vmcam/ssl/rui.crt`

3 Elimine vSphere Authentication Proxy del registro.

   a Vaya al directorio `/usr/lib/vmware-vmcam/bin`, donde se encuentra el script `camregister`.

   b Ejecute el siguiente comando.

```
camregister --unregister -a VC_address -u user
```

   El valor *user* debe ser un usuario de vCenter Single Sign-On que tenga permisos de administrador en vCenter Server.

4 Detenga el servicio de vSphere Authentication Proxy.

Herramienta	Pasos
Interfaz de administración de configuración de vCenter Server	a En un explorador web, desplácese hasta la interfaz de administración de configuración de vCenter Server, https://*dirección-IP-o-FQDN-de-vCenter*:5480. b Inicie sesión como raíz. La contraseña raíz predeterminada es la que estableció al implementar vCenter Server. c Haga clic en **Servicios** y en **VMware vSphere Authentication Proxy**. d Haga clic en **Detener**.
CLI	`service-control --stop vmcam`

5 Reemplace el certificado `rui.crt` existente y los archivos `rui.key` por los archivos que le envió la entidad de certificación.

6 Reinicie el servicio de vSphere Authentication Proxy.

7 Vuelva a registrar vSphere Authentication Proxy explícitamente en vCenter Server usando el nuevo certificado y la clave.

```
camregister --register -a VC_address -u user -c full_path_to_rui.crt -k
full_path_to_rui.key
```

Configurar y administrar la autenticación de tarjeta inteligente para ESXi

Se puede utilizar la autenticación de tarjeta inteligente para iniciar sesión en la interfaz de usuario de la consola directa (Direct Console User Interface, DCUI) de ESXi mediante la comprobación de identidad personal (Personal Identity Verification, PIV), la tarjeta de acceso común (Common Access Card, CAC) o la tarjeta inteligente SC650, en lugar de especificar un nombre de usuario y una contraseña.

Una tarjeta inteligente es una tarjeta plástica pequeña con un chip de circuito integrado. Muchas agencias gubernamentales y empresas grandes utilizan la autenticación en dos fases basada en tarjeta inteligente para incrementar la seguridad de los sistemas y cumplir con las normas de seguridad.

Cuando se habilita la autenticación de tarjeta inteligente en un host ESXi, la DCUI solicita una combinación de tarjeta inteligente y PIN, en lugar de la solicitud predeterminada de nombre de usuario y contraseña.

1 Cuando se introduce la tarjeta inteligente en el lector de tarjetas inteligentes, el host ESXi lee las credenciales de la tarjeta.

2 La DCUI de ESXi muestra su identificador de inicio de sesión y solicita su PIN.

3 Una vez introducido el PIN, el host ESXi busca coincidencias con el PIN almacenado en la tarjeta inteligente y comprueba el certificado en la tarjeta inteligente con Active Directory.

4 Después de la correcta comprobación del certificado de la tarjeta inteligente, ESXi inicia su sesión en la DCUI.

Para pasar a la autenticación mediante nombre de usuario y contraseña desde la DCUI, presione F3.

El chip de la tarjeta inteligente se bloquea después de una serie de ingresos de PIN incorrecto; por lo general, después de tres intentos. Si se bloquea la tarjeta inteligente, únicamente el personal designado puede desbloquearla.

Activar autenticación de tarjeta inteligente

Active la autenticación de tarjeta inteligente para que el sistema solicite la combinación de tarjeta inteligente y PIN para iniciar sesión en la DCUI de ESXi.

Requisitos previos

- Configure la infraestructura para que controle la autenticación de tarjeta inteligente, como cuentas del dominio de Active Directory, lectores de tarjetas inteligentes y tarjetas inteligentes.
- Configure ESXi para que se una a un dominio de Active Directory que admita la autenticación de tarjeta inteligente. Para obtener más información, consulte Usar Active Directory para administrar usuarios de ESXi.
- Utilice vSphere Client para agregar certificados raíz. Consulte Administrar certificados para hosts ESXi.

Procedimiento

1 Desplácese hasta el host en el inventario de vSphere Client.

2 Haga clic en **Configurar**.

3 En Sistema, seleccione **Servicios de autenticación**.

   Puede ver el estado actual de autenticación de tarjeta inteligente y una lista con los certificados importados.

4 En el panel Autenticación de tarjeta inteligente, haga clic en **Editar**.

5 En el cuadro de diálogo Editar autenticación de tarjeta inteligente, seleccione la página Certificados.

6 Agregue certificados de una entidad de certificación (CA) de confianza, por ejemplo, certificados de una CA raíz o intermediaria.

   Los certificados deben estar en formato PEM.

7 Abra la página Autenticación de tarjeta inteligente, active la casilla **Habilitar autenticación de tarjeta inteligente** y haga clic en **Aceptar**.

Desactivar autenticación de tarjeta inteligente

Desactive la autenticación de tarjeta inteligente para regresar a la autenticación predeterminada de nombre de usuario y contraseña que permite iniciar sesión en la DCUI de ESXi.

Procedimiento

1 Desplácese hasta el host en el inventario de vSphere Client.

2 Haga clic en **Configurar**.

3 En Sistema, seleccione **Servicios de autenticación**.

   Puede ver el estado actual de autenticación de tarjeta inteligente y una lista con los certificados importados.

4 En el panel Autenticación de tarjeta inteligente, haga clic en **Editar**.

5 En la página Autenticación de tarjeta inteligente, desactive la casilla **Habilitar autenticación de tarjeta inteligente** y haga clic en **Aceptar**.

Autenticar con nombre de usuario y contraseña en caso de problemas de conectividad

Si no se puede tener acceso al servidor de dominios de Active Directory (AD), puede iniciar sesión en la DCUI de ESXi con la autenticación de nombre de usuario y contraseña para realizar acciones de emergencia en el host.

En raras ocasiones, no se puede tener acceso al servidor de dominio de AD para autenticar las credenciales de usuario en la tarjeta inteligente debido a problemas de conectividad, cortes de red o desastres. En ese caso, puede iniciar sesión en el DCUI de ESXi con las credenciales de un usuario administrador de ESXi local. Después de iniciar sesión, puede realizar diagnósticos u otras acciones de emergencia. La reserva del inicio de sesión con nombre de usuario y contraseña queda registrada. Cuando la conectividad a AD se restaura, se vuelve a habilitar la autenticación de tarjeta inteligente.

Nota La pérdida de la conectividad de red con vCenter Server no afecta la autenticación de tarjeta inteligente si el servidor de Active Directory (AD) está disponible.

Usar la autenticación de tarjeta inteligente en el modo de bloqueo

Cuando el modo de bloqueo está activado en el host ESXi, aumenta la seguridad del host y se limita el acceso a la interfaz de usuario de la consola directa (DCUI). El modo de bloqueo puede hacer que la autenticación de tarjeta inteligente deje de funcionar.

En el modo normal de bloqueo, únicamente los usuarios que figuran en la lista de usuarios con excepción con privilegios de administrador pueden acceder a la DCUI. Los usuarios con excepción son usuarios locales del host o usuarios de Active Directory con permisos definidos localmente para el host ESXi. Si desea utilizar la autenticación de tarjeta inteligente en el modo de bloqueo normal, debe agregar usuarios a la lista de usuarios con excepción desde vSphere Client. Estos usuarios no pierden sus permisos cuando el host entra en el modo de bloqueo normal y pueden iniciar sesión en la DCUI. Para obtener más información, consulte Especificar usuarios con excepción para el modo de bloqueo.

En el modo de bloqueo estricto, el servicio de la DCUI se interrumpe. Como consecuencia, no se puede acceder al host con la autenticación de tarjeta inteligente.

Usar ESXi Shell

ESXi Shell proporciona comandos de mantenimiento esenciales y está desactivado de forma predeterminada en los hosts ESXi. Es posible activar el acceso local y remoto al shell, si es necesario. Para reducir el riesgo de accesos no autorizados, active ESXi Shell solo para solucionar problemas.

ESXi Shell es independiente del modo de bloqueo. Incluso si el host se ejecuta en modo de bloqueo, todavía puede iniciar sesión en ESXi Shell si está activado.

Los servicios aplicables son los siguientes.

ESXi Shell

Active este servicio para acceder a ESXi Shell de forma local.

SSH

Active este servicio para acceder a ESXi Shell de forma remota mediante SSH.

El usuario raíz y los usuarios con la función de administrador pueden acceder a ESXi Shell. Los usuarios que se encuentran en el grupo de Administradores de ESX reciben automáticamente la función de administrador. De forma predeterminada, solamente el usuario raíz puede ejecutar comandos del sistema (como `vmware -v`) mediante ESXi Shell.

Nota No active ESXi Shell a menos que necesite acceder.

Qué leer a continuación

- Establecer el tiempo de espera de inactividad para ESXi Shell mediante vSphere Client

  Si habilita ESXi Shell en un host, pero olvida cerrar la sesión, la sesión inactiva permanece conectada de forma indefinida. La conexión abierta aumenta las posibilidades de que alguien obtenga acceso privilegiado al host. Para impedir esta situación, configure un tiempo de espera para las sesiones inactivas.

- Establecer el tiempo de espera de disponibilidad de ESXi Shell mediante vSphere Client

  ESXi Shell está desactivado de forma predeterminada. Puede establecer un tiempo de espera de disponibilidad para ESXi Shell a fin de aumentar la seguridad cuando se activa el shell.

- Establecer el tiempo de espera de disponibilidad o el tiempo de espera de inactividad para ESXi Shellmediante la DCUI

  ESXi Shell está desactivado de forma predeterminada. Para aumentar la seguridad cuando se activa el shell, puede establecer un tiempo de espera de disponibilidad, un tiempo de espera de inactividad o ambos.

- Activar el acceso a ESXi Shell mediante vSphere Client

  ESXi Shell y las interfaces SSH están desactivados de forma predeterminada. Mantenga estas interfaces desactivadas a menos que esté realizando actividades de solución de problemas o de soporte. Para las actividades cotidianas, utilice vSphere Client, donde la actividad está sujeta al control de acceso basado en roles y a métodos de control de acceso modernos.

- Activar el acceso a ESXi Shell mediante la DCUI

  La interfaz de usuario de la consola directa (DCUI) permite interactuar con el host de forma local mediante los menús basados en texto. Determine si los requisitos de seguridad de su entorno admiten la activación de la interfaz de usuario de la consola directa.

- Iniciar sesión en ESXi Shell para solucionar problemas

  Realice tareas de configuración de ESXi con vSphere Client, ESXCLI o VMware PowerCLI. Inicie sesión en ESXi Shell (anteriormente Tech Support Mode o TSM) solo para fines de solución de problemas.

Establecer el tiempo de espera de inactividad para ESXi Shell mediante vSphere Client

Si habilita ESXi Shell en un host, pero olvida cerrar la sesión, la sesión inactiva permanece conectada de forma indefinida. La conexión abierta aumenta las posibilidades de que alguien obtenga acceso privilegiado al host. Para impedir esta situación, configure un tiempo de espera para las sesiones inactivas.

El tiempo de espera de inactividad corresponde a la cantidad de tiempo que puede transcurrir antes de que se cierre la sesión interactiva inactiva de un usuario. Es posible controlar la cantidad de tiempo que duran una sesión local y una sesión remota (SSH) desde la interfaz de usuario de la consola directa (DCUI) o desde vSphere Client.

Procedimiento

1 Desplácese hasta el host en el inventario de vSphere Client.

2 Haga clic en **Configurar**.

3 En Sistema, seleccione **Configuración avanzada del sistema**.

4 Haga clic en **Editar**, seleccione `UserVars.ESXiShellInteractiveTimeOut` e introduzca la configuración de tiempo de espera.

   Un valor de cero (0) desactiva el tiempo de inactividad.

5 Reinicie el servicio de ESXi Shell y el servicio SSH para que se aplique el tiempo de espera.

   a Vaya a **Sistema > Servicios**.

   b Uno a uno, seleccione ESXi Shell y SSH, y haga clic en **Reiniciar**.

Resultados

Si la sesión está inactiva, se cerrará la sesión de los usuarios una vez transcurrido el período de tiempo de espera.

Establecer el tiempo de espera de disponibilidad de ESXi Shell mediante vSphere Client

ESXi Shell está desactivado de forma predeterminada. Puede establecer un tiempo de espera de disponibilidad para ESXi Shell a fin de aumentar la seguridad cuando se activa el shell.

La configuración de tiempo de espera de disponibilidad corresponde a la cantidad de tiempo que puede transcurrir antes de que pueda iniciar sesión tras la activación de ESXi Shell. Una vez que transcurre el período de espera, el servicio se desactiva y los usuarios no pueden iniciar sesión.

Procedimiento

1 Desplácese hasta el host en el inventario de vSphere Client.

2 Haga clic en **Configurar**.

3 En Sistema, seleccione **Configuración avanzada del sistema**.

4 Haga clic en **Editar** y seleccione `UserVars.ESXiShellTimeOut`.

5 Introduzca la configuración de tiempo de espera de inactividad.

6 Haga clic en **Aceptar**.

7 Reinicie el servicio de ESXi Shell y el servicio SSH para que se aplique el tiempo de espera.

   a Vaya a **Sistema > Servicios**.

   b Uno a uno, seleccione ESXi Shell y SSH, y haga clic en **Reiniciar**.

Resultados

Si inicia sesión y se agota el tiempo de espera, la sesión se mantiene activa. No obstante, una vez que se cierra o se interrumpe la sesión, los usuarios no pueden iniciar sesión.

Establecer el tiempo de espera de disponibilidad o el tiempo de espera de inactividad para ESXi Shellmediante la DCUI

ESXi Shell está desactivado de forma predeterminada. Para aumentar la seguridad cuando se activa el shell, puede establecer un tiempo de espera de disponibilidad, un tiempo de espera de inactividad o ambos.

Los dos tipos de tiempo de espera se aplican en situaciones diferentes.

Tiempo de espera de inactividad de ESXi Shell

Si un usuario activa ESXi Shell en un host, pero olvida cerrar la sesión, la sesión inactiva permanece conectada de forma indefinida. La conexión abierta puede aumentar la posibilidad de que alguien obtenga acceso privilegiado al host. Para evitar que esta situación se produzca, configure un tiempo de espera de las sesiones inactivas.

Tiempo de espera de disponibilidad de ESXi Shell

El tiempo de espera de disponibilidad determina cuánto tiempo puede transcurrir antes de iniciar sesión después de activar el shell inicialmente. Si espera más tiempo, el servicio se desactiva y ya no se puede iniciar sesión en ESXi Shell.

Requisitos previos

Active ESXi Shell. Consulte Activar el acceso a ESXi Shell mediante la DCUI.

Procedimiento

1 Inicie sesión en ESXi Shell.

2 En el menú Opciones del modo de solución de problemas, seleccione **Modificar tiempos de espera de SSH y ESXi Shell** y presione Intro.

3 Introduzca el tiempo de espera de inactividad (en segundos) o el tiempo de espera de disponibilidad.

4 Presione Entrar y Esc hasta regresar al menú principal de la interfaz de usuario de la consola directa.

5 Haga clic en **Aceptar**.

6 Reinicie el servicio de ESXi Shell y el servicio SSH para que se aplique el tiempo de espera.

   a En vSphere Client, seleccione el host y vaya a **Configurar > Sistema > Servicios**.

   b Uno a uno, seleccione ESXi Shell y SSH, y haga clic en **Reiniciar**.

Resultados

- Si establece el tiempo de espera de inactividad, se desconecta a los usuarios una vez que la sesión está inactiva durante el tiempo especificado.
- Si establece el tiempo de espera de disponibilidad y no inicia sesión antes de que transcurra ese tiempo de espera, los inicios de sesión se vuelven a desactivar.

Activar el acceso a ESXi Shell mediante vSphere Client

ESXi Shell y las interfaces SSH están desactivados de forma predeterminada. Mantenga estas interfaces desactivadas a menos que esté realizando actividades de solución de problemas o de soporte. Para las actividades cotidianas, utilice vSphere Client, donde la actividad está sujeta al control de acceso basado en roles y a métodos de control de acceso modernos.

Nota Acceda al host con vSphere Client, con herramientas de línea de comandos remotas (ESXCLI y PowerCLI) y con las API publicadas. No active el acceso remoto al host mediante SSH a menos que circunstancias especiales lo requieran.

Requisitos previos

Si desea utilizar una clave de SSH autorizada, puede cargarla. Consulte Claves SSH de ESXi.

Procedimiento

1 Desplácese hasta el host en el inventario.

2 En Sistema, haga clic en **Configurar** y, a continuación, en **Servicios**.

3 Administre los servicios de ESXi, SSH o interfaz de usuario de consola directa.

   a En el panel Servicios, seleccione el servicio.

   b Haga clic en **Editar directiva de inicio** y seleccione la directiva de inicio **Iniciar y detener manualmente**.

   c Para activar el servicio, haga clic en **Iniciar**.

   Cuando se selecciona **Iniciar y detener manualmente**, el servicio no se inicia al reiniciar el host. Si desea que el servicio se inicie al reiniciar el host, seleccione **Iniciar y detener con el host**.

Pasos siguientes

Establezca los tiempos de espera de disponibilidad e inactividad para ESXi Shell. Consulte Establecer el tiempo de espera de disponibilidad de ESXi Shell mediante vSphere Client y Establecer el tiempo de espera de inactividad para ESXi Shell mediante vSphere Client.

Activar el acceso a ESXi Shell mediante la DCUI

La interfaz de usuario de la consola directa (DCUI) permite interactuar con el host de forma local mediante los menús basados en texto. Determine si los requisitos de seguridad de su entorno admiten la activación de la interfaz de usuario de la consola directa.

Se puede utilizar la interfaz de usuario de la consola directa (DCUI) para activar el acceso local y remoto a ESXi Shell. A la interfaz de usuario de la consola directa se accede desde la consola física asociada al host. Después de que el host se reinicie y cargue ESXi, pulse F2 para iniciar sesión en la DCUI. Introduzca las credenciales que creó cuando instaló ESXi.

Nota Los cambios que se realizan en el host desde la interfaz de usuario de la consola directa, vSphere Client, ESXCLI u otras herramientas administrativas se envían al almacenamiento permanente cada una hora o después de un apagado correcto. Si se produce un error en el host antes de que los cambios se confirmen, estos podrían perderse.

Procedimiento

1 En la interfaz de usuario de la consola directa, presione F2 para acceder al menú Personalización del sistema.

2 Seleccione **Opciones de solución de problemas** y presione Intro.

3 En el menú Opciones del modo de solución de problemas, seleccione un servicio para activar.

   - Habilitar ESXi Shell
   - Habilitar SSH

4 Presione Intro para activar el servicio.

5 Presione Esc hasta que vuelva al menú principal de la interfaz de usuario de la consola directa.

Pasos siguientes

Establezca los tiempos de espera de disponibilidad e inactividad para ESXi Shell. Consulte Establecer el tiempo de espera de disponibilidad o el tiempo de espera de inactividad para ESXi Shellmediante la DCUI.

Iniciar sesión en ESXi Shell para solucionar problemas

Realice tareas de configuración de ESXi con vSphere Client, ESXCLI o VMware PowerCLI. Inicie sesión en ESXi Shell (anteriormente Tech Support Mode o TSM) solo para fines de solución de problemas.

Procedimiento

1 Inicie sesión en ESXi Shell con uno de los siguientes métodos.

   - Si tiene acceso directo al host, presione Alt + F1 para abrir la página de inicio de sesión en la consola física de la máquina.

- Si se conecta al host de forma remota, utilice SSH u otra conexión de consola remota para iniciar una sesión en el host.

2 Escriba un nombre de usuario y una contraseña que reconozca el host.

Arranque seguro UEFI para hosts ESXi

El arranque seguro forma parte del estándar de firmware UEFI. Al utilizar el arranque seguro, una máquina se niega a cargar cualquier controlador UEFI o aplicación, salvo que el cargador de arranque del sistema operativo esté firmado con datos de cifrado. En vSphere 6.5 y versiones posteriores, ESXi admite el arranque seguro si está habilitado en el hardware.

Cómo ESXi utiliza el arranque seguro UEFI

ESXi 6.5 y las versiones posteriores admiten el arranque seguro UEFI en cada nivel de la pila de arranque.

Nota Antes de usar el arranque seguro UEFI en un host que se haya actualizado, siga las instrucciones en Ejecutar el script de validación de arranque seguro después de la actualización de ESXi para verificar la compatibilidad.

Figura 3-1. arranque seguro UEFI

Al utilizar el arranque seguro, la secuencia de arranque es la que se describe a continuación.

1 En vSphere 6.5 y versiones posteriores, el cargador de arranque de ESXi contiene una clave pública de VMware. El cargador de arranque utiliza la clave para verificar la firma del kernel y un subconjunto pequeño del sistema que incluye un verificador VIB de arranque seguro.

2 El verificador VIB verifica cada paquete VIB que se instala en el sistema.

En este punto, todo el sistema arranca con la raíz de confianza en los certificados que son parte del firmware UEFI.

Nota Cuando instala o actualiza a vSphere 7.0 Update 2 o a una versión posterior y un host ESXi tiene un TPM, el TPM sella la información confidencial mediante una directiva de TPM basada en valores de PCR para el arranque seguro UEFI. Este valor se carga durante los reinicios posteriores si se cumple la directiva como verdadera. Para saber cómo desactivar o activar el arranque seguro UEFI en vSphere 7.0 Update 2 o una versión posterior, consulte Activar o desactivar la aplicación del arranque seguro para una configuración de ESXi segura.

Solución de problemas del arranque seguro UEFI

Si no se logra un arranque seguro en ningún nivel de la secuencia de arranque, se produce un error.

El mensaje de error depende del proveedor de hardware y del nivel en el que no se pudo realizar la verificación.

- Si intenta arrancar con un cargador de arranque no firmado o alterado, se produce un error durante la secuencia de arranque. El mensaje exacto depende del proveedor de hardware. Se puede parecer al siguiente error o ser diferente.

```
UEFI0073: Unable to boot PXE Device...because of the Secure Boot policy
```

- Si se alteró el kernel, se produce un error como el siguiente.

```
Fatal error: 39 (Secure Boot Failed)
```

- Si se alteró un paquete (VIB o controlador), se muestra una pantalla violeta con el siguiente mensaje.

```
UEFI Secure Boot failed:
Failed to verify signatures of the following vibs (XX)
```

Para resolver problemas con el arranque seguro, siga estos pasos.

1 Reinicie el host con el arranque seguro desactivado.

2 Ejecute el script de verificación de arranque seguro (consulte Ejecutar el script de validación de arranque seguro después de la actualización de ESXi).

3 Examine la información en el archivo `/var/log/esxupdate.log`.

Ejecutar el script de validación de arranque seguro después de la actualización de ESXi

Después de actualizar un host ESXi desde una versión que no admite el arranque seguro UEFI, debe comprobar si puede activar el arranque seguro.

Para que el arranque seguro se realice correctamente, la firma de cada VIB instalado debe estar disponible en el sistema. Las versiones anteriores de ESXi no guardan las firmas cuando se instalan los VIB.

- Si realiza la actualización mediante comandos ESXCLI, la versión anterior de ESXi instalará los nuevos VIB, por lo que no se guardarán las firmas y no será posible realizar el arranque seguro.
- Si realiza la actualización mediante el archivo ISO, se guardarán las firmas de los nuevos VIB. Esto también es así para las actualizaciones de vSphere Lifecycle Manager que utilicen el archivo ISO.
- Si los VIB anteriores permanecen en el sistema, las firmas de dichos VIB no estarán disponibles y no será posible realizar el arranque seguro.
  - Si el sistema utiliza un controlador de terceros y la actualización de VMware no incluye una nueva versión del VIB de controlador, el VIB anterior permanecerá en el sistema tras la actualización.
  - En casos excepcionales, VMware puede descartar el desarrollo en curso de un VIB específico sin proporcionar un nuevo VIB que lo reemplace o lo deje obsoleto, de manera que el VIB anterior permanece en el sistema tras la actualización.

Nota El arranque seguro UEFI también requiere un cargador de arranque actualizado. Este script no comprueba que haya un cargador de arranque actualizado.

Requisitos previos

Después de actualizar un host ESXi a partir de una versión anterior de ESXi que no admitía el arranque seguro UEFI, es posible que pueda activar el arranque seguro. La posibilidad de activar el arranque seguro depende de la forma en la que se haya hecho la actualización y de si esta reemplazó todos los VIB existentes o dejó alguno sin modificar. Puede ejecutar el script de validación después de realizar la actualización para determinar si la instalación actualizada admite el arranque seguro.

- Verifique que el hardware admita el arranque seguro UEFI.
- Verifique que todos los VIB estén firmados con un nivel de aceptación PartnerSupported, como mínimo. Si incluye VIB en el nivel CommunitySupported, no podrá usar el arranque seguro.

Procedimiento

1 Actualice ESXi y ejecute el siguiente comando.

```
/usr/lib/vmware/secureboot/bin/secureBoot.py -c
```

2 Compruebe el resultado.

El resultado incluye `Secure boot can be enabled` o `Secure boot CANNOT be enabled`.

Proteger hosts ESXi con el módulo de plataforma de confianza

Los hosts ESXi pueden utilizar los chips de los módulos de plataforma de confianza (Trusted Platform Module, TPM), los cuales son procesadores criptográficos seguros que mejoran la seguridad de los hosts, ya que proporcionan una garantía de confianza con acceso raíz en el hardware en lugar de en el software.



(Demostración de la característica de ESXi y Trusted Platform Module 2.0)

Qué es TPM

TPM es un estándar de la industria para los procesadores criptográficos seguros. Actualmente, los chips TPM se utilizan en la mayoría de los equipos, desde portátiles hasta equipos de escritorio y servidores. vSphere 6.7 y las versiones posteriores son compatibles con la versión 2.0 de TPM.

Un chip TPM 2.0 atesta una identidad de ESXi de un host. La atestación de host es el proceso que se sigue para autenticar y avalar el estado del software de un host en un momento específico. El arranque seguro UEFI, por el cual solo se carga software firmado en el arranque, es un requisito para la atestación exitosa. El chip TPM 2.0 registra y almacena de forma segura las mediciones de los módulos de software arrancados en el sistema, lo que vCenter Server verifica de forma remota.

Los pasos de alto nivel del proceso de atestación remota son:

1 Establecer la confiabilidad del TPM remoto y crear una clave de atestación (Attestation Key, AK) en el módulo.

   Cuando un host ESXi se agrega a, se reinicia desde o se vuelve a conectar a vCenter Server, vCenter Server solicita una AK del host. Una parte del proceso de creación de AK también implica la verificación del hardware de TPM para garantizar que lo haya producido un proveedor conocido (y de confianza).

2 Recuperar el informe de atestación del host.

   vCenter Server solicita que el host envíe un informe de atestación, el cual incluye una oferta de los registros de configuración de la plataforma (Platform Configuration Registers, PCR), firmada por TPM, y otros metadatos binarios de host firmados. Al comprobar que la información corresponde a una configuración que se considera de confianza, una instancia de vCenter Server identifica la plataforma en un host que anteriormente no era de confianza.

3 Compruebe la autenticidad del host.

   vCenter Server verifica la autenticidad de la oferta firmada, deduce las versiones de software y determina la confiabilidad de las versiones de dicho software. Si vCenter Server determina que la oferta firmada no es válida, se produce un error en la atestación remota y el host no se considera de confianza.

Cuáles son los requisitos de vSphere para usar un TPM

Para utilizar un chip TPM 2.0, el entorno de vCenter Server debe cumplir estos requisitos:

- vCenter Server 6.7 o versiones posteriores
- Host ESXi 6.7 o versión posterior con un chip TPM 2.0 instalado y habilitado en UEFI
- Arranque seguro UEFI habilitado

Asegúrese de que TPM esté configurado en el BIOS del host ESXi para utilizar el algoritmo de hash SHA-256 y la interfaz TIS/FIFO (First-In, First-Out), y no CRB (Command Response Buffer). Para obtener más información acerca de cómo configurar las opciones de la BIOS necesarias, consulte la documentación del proveedor.

Consulte los chips TPM 2.0 certificados por VMware en la siguiente ubicación:

https://www.vmware.com/resources/compatibility/search.php

Qué sucede al arrancar un host con TPM

Al arrancar un host ESXi con un chip TPM 2.0 instalado, vCenter Server supervisa el estado de atestación del host. Para ver el estado de confianza del hardware, en vSphere Client, seleccione vCenter Server y, a continuación, la pestaña **Resumen** en **Supervisar**. El estado de confianza del hardware es uno de los siguientes:

- Verde: estado Normal, es decir, plena confianza.
- Rojo: no se pudo atestar.

Nota Si agrega un chip TPM 2.0 a un host ESXi que ya administra vCenter Server, primero debe desconectar el host y, a continuación, volver a conectarlo. Consulte la documentación de *Administrar vCenter Server y hosts* para obtener más información sobre cómo desconectar y volver a conectar hosts.

Con vSphere 7.0 y versiones posteriores, VMware® vSphere Trust Authority™ utiliza funcionalidades de atestación remota para hosts ESXi. Consulte Qué es el servicio de atestación de vSphere Trust Authority.

Ver el estado de atestación de un host ESXi

Cuando se agrega a un host ESXi, un chip compatible con Trusted Platform Module 2.0 atesta la integridad de la plataforma. Puede ver el estado de atestación del host en vSphere Client. También puede ver el estado de la tecnología de ejecución de confianza (Trusted Execution Technology, TXT) de Intel.

Procedimiento

1. Conéctese a vCenter Server mediante vSphere Client.
2. Desplácese hasta un centro de datos y haga clic en la pestaña **Supervisar**.
3. Haga clic en **Seguridad**.

4 Revise el estado del host en la columna Atestación y lea el mensaje adjunto en la columna **Mensaje**.

5 Si este host es un host de confianza, consulte Ver el estado de atestación de un clúster de confianza para obtener más información.

Pasos siguientes

Si el estado de atestación es Error o Advertencia, consulte Solucionar problemas de atestación de host ESXi. Para los hosts de confianza, consulte Solucionar problemas de atestación de host de confianza.

Solucionar problemas de atestación de host ESXi

Cuando se instala un dispositivo con módulo de plataforma de confianza (Trusted Platform Module, TPM) en un host ESXi, es posible que este no pase la atestación. Puede solucionar las posibles causas de este problema.

Procedimiento

1 Puede ver el estado de la alarma del host ESXi y el correspondiente mensaje de error. Consulte Ver el estado de atestación de un host ESXi.

2 Si el mensaje de error es `Arranque seguro de host deshabilitado`, debe volver a habilitar el arranque seguro para resolver el problema.

3 Si se produce un error en el estado de atestación del host, busque el siguiente mensaje en el archivo `vpxd.log` de vCenter Server:

```
No hay ninguna clave de identidad en la memoria caché; se cargará de la base de datos
```

Este mensaje indica que se está agregando un chip TPM 2.0 a un host de ESXi que ya administra vCenter Server. En primer lugar, debe desconectar el host y, a continuación, volver a conectarlo. Consulte la documentación de *Administrar vCenter Server y hosts* para obtener más información sobre cómo desconectar y reconectar hosts.

Para obtener más información sobre los archivos de registro de vCenter Server, incluidas la ubicación y la rotación de registros, consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/1021804.

4 Para todos los demás mensajes es de error, póngase en contacto con soporte al cliente.

Archivos de registro de ESXi

Los archivos de registro son un componente importante para la solución de problemas de ataques y la obtención de información sobre las vulneraciones. Todos los hosts de ESXi ejecutan un servicio syslog, que registra mensajes del VMkernel y otros componentes del sistema en archivos locales o en un host remoto.

Para aumentar la seguridad del host, tome las siguientes medidas:

- Configure los registros persistentes en un almacén de datos. De forma predeterminada, los registros en los hosts ESXi se almacenan en el sistema de archivos en la memoria. Por lo tanto, se pierden con cada reinicio del host y solo se almacenan 24 horas de datos de registros. Al habilitar los registros persistentes, tiene un registro dedicado de la actividad para el host.
- El registro remoto a un host central permite recopilar archivos de registro en un host central. Desde ese host, puede supervisar todos los hosts con una sola herramienta, realizar análisis agregados y buscar datos de registros. Este enfoque facilita la supervisión y revela información sobre ataques coordinados en varios hosts.
- Utilice ESXCLI, PowerCLI o un cliente API para configurar syslog remoto seguro en hosts ESXi.
- Consulte la configuración de syslog para asegurarse de que el puerto y el servidor syslog sean válidos.

Consulte la documentación de *Supervisión y rendimiento de vSphere* para obtener información sobre la configuración de syslog y sobre los archivos de registro de ESXi.

Configurar Syslog en hosts ESXi

Puede utilizar vSphere Client, VMware Host Client o el comando `esxcli system syslog` para configurar el servicio syslog.

Para obtener información sobre cómo utilizar el comando `esxcli system syslog` y otros comandos ESXCLI, consulte *Introducción a ESXCLI*. Para obtener más información sobre cómo abrir el firewall de ESXi para el puerto especificado en cada especificación de host remoto, consulte Configurar el firewall de ESXi.

Procedimiento

1. Desplácese hasta el host en el inventario de vSphere Client.
2. Haga clic en **Configurar**.
3. En **Sistema**, haga clic en **Configuración avanzada del sistema**.
4. Haga clic en **Editar**.
5. Filtre por **`syslog`**.
6. Para configurar globalmente el registro y configurar varias opciones avanzadas, consulte Opciones de Syslog de ESXi.
7. (opcional) Para sobrescribir los valores predeterminados de tamaño de registro y rotación de registros de cualquier registro:
   a. Haga clic en el nombre del registro que desea personalizar.
   b. Introduzca el número de rotaciones y el tamaño de registro que desea.
8. Haga clic en **Aceptar**.

Resultados

Los cambios en las opciones de syslog surten efecto.

Nota La configuración de parámetros de syslog que se define mediante vSphere Client o VMware Host Client se aplica inmediatamente. Sin embargo, la mayoría de los ajustes que se definen mediante ESXCLI requieren un comando adicional para que surtan efecto. Para obtener más información, consulte Opciones de Syslog de ESXi.

Opciones de Syslog de ESXi

Puede definir el comportamiento de las transmisiones y los archivos de syslog de ESXi mediante un conjunto de opciones de syslog.

Además de la configuración básica, como `Syslog.global.logHost`, a partir de ESXi 7.0 Update 1, hay disponible una lista de opciones avanzadas para las personalizaciones y el cumplimiento de NIAP.

Nota Configure siempre el almacenamiento persistente antes de establecer alguno de los parámetros de registro de auditoría o el parámetro de `Syslog.global.logDir`.

Nota Todos los ajustes del registro de auditoría que comienzan por `Syslog.global.auditRecord` se aplican inmediatamente. Sin embargo, para otros ajustes que defina mediante ESXCLI, asegúrese de ejecutar el comando `esxcli system syslog reload` para habilitar los cambios.

Tabla 3-9. Opciones de Syslog heredadas

Opción	Comando ESXCLI	Descripción
`Syslog.global.logHost`	`esxcli system syslog config set --loghost=<str>`	Define una lista delimitada por comas de hosts remotos y especificaciones para transmisiones de mensajes. Si el campo `loghost=<str>` está en blanco, no se reenvía ningún registro. Si bien no existe un límite estricto para la cantidad de hosts remotos que recibirán mensajes de Syslog, una buena práctica es mantener el número de hosts remotos en cinco o menos. El formato de una especificación de host remoto es: `protocol://hostname|ipv4|'['ipv6']'[:port]`. El protocolo debe ser TCP, UDP o SSL. El valor de los puertos puede ser cualquier número decimal entre 1 y 65535. Si no se proporciona un puerto, SSL y TCP utilizan 1514. UDP utiliza 514. Por ejemplo: `ssl://hostName1:1514`.
`Syslog.global.defaultRotate`	`esxcli system syslog config set --default-rotate=<long>`	Número máximo de archivos de registro antiguos que se conservarán. Puede configurar este número en forma global y para subregistradores individuales (consulte `Syslog.global.defaultSize`).
`Syslog.global.defaultSize`	`esxcli system syslog config set --default-size=<long>`	Tamaño predeterminado de los archivos de registro, en KiB. Una vez que un archivo alcanza el tamaño predeterminado, el servicio de Syslog crea un nuevo archivo. Puede configurar este número en forma global y para subregistradores individuales.

Tabla 3-9. Opciones de Syslog heredadas (continuación)

Opción	Comando ESXCLI	Descripción
Syslog.global.logDir	esxcli system syslog config set --logdir=<str>	Directorio donde residen los registros. El directorio puede encontrarse en volúmenes NFS o VMFS montados. Solo el directorio /scratch del sistema de archivos local se mantiene en todos los reinicios. Especifique el directorio como [*nombrealmacéndatos*] *ruta_a_archivo*, donde la ruta de acceso es relativa a la raíz del volumen que respalda el almacén de datos. Por ejemplo, la ruta de acceso [storage1] /systemlogs se asigna a la ruta de acceso /vmfs/volumes/storage1/systemlogs.
Syslog.global.logDirUnique	esxcli system syslog config set --logdir-unique=<bool>	Especifica el nombre de host ESXi que se va a concatenar al valor de Syslog.global.logDir. Es fundamental que habilite esta opción cuando varios hosts ESXi inicien sesión en un sistema de archivos compartido. Al seleccionar esta opción, se crea un subdirectorio con el nombre del host ESXi del directorio especificado por **Syslog.global.LogDir**. Un directorio único es útil si varios hosts ESXi utilizan el mismo directorio NFS.
Syslog.global.certificate.checkSSLCerts	esxcli system syslog config set --check-ssl-certs=<bool>	Examine la comprobación de certificados SSL al transmitir mensajes a hosts remotos.

Tabla 3-10. Opciones de Syslog disponibles a partir de ESXi 7.0 Update 1

Opción	Comando ESXCLI	Descripción
Syslog.global.auditRecord.storageCapacity	esxcli system auditrecords local set --size=<long>	Especifica la capacidad del directorio de almacenamiento de registros de auditoría ubicado en el host ESXi, en MiB. No se puede reducir la capacidad del almacenamiento de registros de auditoría. Puede aumentar la capacidad antes o después de habilitar el almacenamiento de registros de auditoría (consulte Syslog.global.auditRecord.storageEnable).

Tabla 3-10. Opciones de Syslog disponibles a partir de ESXi 7.0 Update 1 (continuación)

Opción	Comando ESXCLI	Descripción
`Syslog.global.auditRecord.remoteEnable`	`esxcli system auditrecords remote enable`	Habilita el envío de registros de auditoría a hosts remotos. Los hosts remotos se especifican mediante el parámetro `Syslog.global.logHost`.
`Syslog.global.auditRecord.storageDirectory`	`esxcli system auditrecords local set --directory=<dir>`	Crea un directorio de almacenamiento de registros de auditoría y, a menos que se especifique, establece `/scratch/auditLog` como la ubicación predeterminada. No debe crear manualmente un directorio de almacenamiento de registros de auditoría y no puede cambiar el directorio de almacenamiento de registros de auditoría mientras esté habilitado el almacenamiento de registros de auditoría (consulte `Syslog.global.auditRecord.storageEnable`).
`Syslog.global.auditRecord.storageEnable`	`esxcli system auditrecords local enable`	Habilita el almacenamiento de registros de auditoría en un host ESXi. Si el directorio de almacenamiento de registros de auditoría no existe, se crea con la capacidad especificada por `Syslog.global.auditRecord.storageCapacity`.
`Syslog.global.certificate.checkCRL`	`esxcli system syslog config set --crl-check=<bool>`	Habilita la comprobación del estado de revocación de todos los certificados de una cadena de certificados SSL. Habilita la verificación de las CRL X.509 que no se comprueban de forma predeterminada en cumplimiento de las convenciones del sector. Una configuración validada por NIAP requiere comprobaciones de CRL. Debido a las limitaciones de implementación, si se habilitan las comprobaciones de CRL, todos los certificados de una cadena de certificados deben proporcionar un vínculo de CRL. No habilite la opción `crl-check` para instalaciones no relacionadas con la certificación, debido a la dificultad de configurar correctamente un entorno que utilice comprobaciones de CRL.

Tabla 3-10. Opciones de Syslog disponibles a partir de ESXi 7.0 Update 1 (continuación)

Opción	Comando ESXCLI	Descripción
Syslog.global.certificate.strictX509Compliance	esxcli system syslog config set --x509-strict=<bool>	Habilita la conformidad estricta con X.509. Realiza comprobaciones de validez adicionales en los certificados raíz de CA durante la verificación. Por lo general, estas comprobaciones no se realizan, ya que las raíces de CA son de confianza inherente y podrían producir incompatibilidades con las raíces de CA existentes y mal configuradas. Una configuración validada por NIAP requiere que incluso las raíces de CA pasen las validaciones. No habilite la opción x509-strict para instalaciones no relacionadas con la certificación, debido a la dificultad de configurar correctamente un entorno que utilice comprobaciones de CRL.
Syslog.global.droppedMsgs.fileRotate	esxcli system syslog config set --drop-log-rotate=<long>	Especifica el número de archivos antiguos de registro de mensajes descartados que se conservarán.
Syslog.global.droppedMsgs.fileSize	esxcli system syslog config set --drop-log-size=<long>	Especifica el tamaño de cada archivo de registro de mensajes descartados antes de cambiar a uno nuevo, en KiB.
Syslog.global.logCheckSSLCerts	esxcli system syslog config set --check-ssl-certs=<bool>	Examine la comprobación de certificados SSL al transmitir mensajes a hosts remotos. **Nota** Obsoleto. Use Syslog.global.certificate.checkSSLCerts en ESXi 7.0 Update 1 y posterior.

Tabla 3-10. Opciones de Syslog disponibles a partir de ESXi 7.0 Update 1 (continuación)

<table>
<tr><th>Opción</th><th>Comando ESXCLI</th><th>Descripción</th></tr>
<tr><td>Syslog.global.logFilters</td><td>esxcli system syslog config logfilter [add | remove | set] ...</td><td>Especifica una o varias especificaciones de filtrado de registros. Cada filtro de registro debe estar separado por una barra vertical doble (||). El formato de los filtros de registro es: numLogs | ident | logRegexp. numLogs establece la cantidad máxima de entradas de registro para los mensajes de registro especificados. Una vez alcanzado este número, se filtran y se omiten los mensajes de registro especificados. ident especifica uno o más componentes del sistema para aplicar el filtro a los mensajes de registro que generan estos componentes. logRegexp especifica una frase que distingue mayúsculas de minúsculas con la sintaxis de la expresión regular Python para filtrar los mensajes de registro según su contenido.</td></tr>
<tr><td>Syslog.global.logFiltersEnable</td><td></td><td>Habilita el uso de filtros de registro.</td></tr>
<tr><td>Syslog.global.logLevel</td><td>esxcli system syslog config set --log-level=<str></td><td>Especifica el nivel de filtrado de registros. Debe cambiar este parámetro solo para solucionar problemas relacionados con el daemon de syslog. Puede utilizar los valores debug para el nivel más detallado, info para el nivel de detalle predeterminado, warning solo para advertencias o errores, o error solo para errores.</td></tr>
<tr><td>Syslog.global.msgQueueDropMark</td><td>esxcli system syslog config --queue-drop-mark=<long>)</td><td>Especifica el porcentaje de la capacidad de la cola de mensajes a partir del cual se descartan los mensajes.</td></tr>
<tr><td>Syslog.global.remoteHost.connectRetryDelay</td><td>esxcli system syslog config set --default-timeout=<long></td><td>Especifica el retraso antes de volver a intentar conectarse a un host remoto después de que se haya producido un error en un intento de conexión, en segundos.</td></tr>
</table>

Tabla 3-10. Opciones de Syslog disponibles a partir de ESXi 7.0 Update 1 (continuación)

Opción	Comando ESXCLI	Descripción
Syslog.global.remoteHost.maxMsgLen	esxcli system syslog config set --remote-host-max-msg-len=<long>	Para los protocolos TCP y SSL, este parámetro especifica la longitud máxima de una transmisión de Syslog antes de que se produzca truncamiento, en bytes. La longitud máxima predeterminada para los mensajes de host remoto es 1 KiB. Puede aumentar la longitud máxima del mensaje hasta 16 KiB. No obstante, aumentar este valor por encima de 1 KiB no garantiza que las transmisiones largas lleguen sin truncar a un recopilador de Syslog. Por ejemplo, cuando la infraestructura de syslog que emite un mensaje es externa a ESXi. Esta configuración no afecta al protocolo UDP. RFC 5426 establece la longitud máxima de transmisión de mensajes para el protocolo UDP en 480 bytes para IPV4 y 1180 bytes para IPV6. Debido a esta restricción, y debido a que la infraestructura de redes puede descartar de forma arbitraria los paquetes UDP, no se recomienda el uso de UDP para transmitir mensajes críticos de Syslog.
Syslog.global.vsanBacking	esxcli system syslog config set --vsan-backing=<bool>	Permite que los archivos de registro y el directorio de almacenamiento de registros de auditoría se coloquen en un clúster de vSAN. Sin embargo, si se habilita este parámetro, es posible que el host ESXi deje de responder.

Ubicaciones de archivos de registro de ESXi

ESXi registra la actividad de los hosts en los archivos de registro, mediante una funcionalidad de Syslog.

Tabla 3-11. Ubicaciones de archivos de registro de ESXi

Componente	Ubicación	Propósito
Autenticación	/var/log/auth.log	Contiene todos los eventos relacionados con la autenticación para el sistema local.
Registro del agente del host ESXi	/var/log/hostd.log	Contiene información sobre el agente que administra y configura el host ESXi y sus máquinas virtuales.

Tabla 3-11. Ubicaciones de archivos de registro de ESXi (continuación)

Componente	Ubicación	Propósito
Registro del shell	`/var/log/shell.log`	Contiene un registro de todos los comandos introducidos en ESXi Shell y los eventos del shell (por ejemplo, el momento en que se habilitó el shell).
Mensajes del sistema	`/var/log/syslog.log`	Contiene todos los mensajes del registro general y puede usarse para solución de problemas. Esta información antes se encontraba en los mensajes del archivo de registro.
Registro del agente de vCenter Server	`/var/log/vpxa.log`	Contiene información sobre el agente que se comunica con vCenter Server (si el host lo administra vCenter Server).
Máquinas virtuales	El mismo directorio en el que se encuentran los archivos de configuración de la máquina virtual afectada, denominados `vmware.log` y `vmware*.log`. Por ejemplo, `/vmfs/volumes/datastore/virtual machine/vmware.log`	Contiene todos los eventos relacionados con el encendido de la máquina virtual, la información de errores del sistema, la actividad y el estado de las herramientas, la sincronización de hora, los cambios en el hardware virtual, las migraciones de vMotion, los clones de la máquina, etc.
VMkernel	`/var/log/vmkernel.log`	Registra las actividades relacionadas con máquinas virtuales y ESXi.
Resumen de VMkernel	`/var/log/vmksummary.log`	Se utiliza para determinar las estadísticas de disponibilidad y tiempo de actividad de ESXi (valores separados por comas).
Advertencias de VMkernel	`/var/log/vmkwarning.log`	Registra las actividades relacionadas con máquinas virtuales.
Quick Boot	`/var/log/loadESX.log`	Contiene todos los eventos relacionados con el reinicio de un host ESXi a través de Quick Boot.
Agente de infraestructura de confianza	`/var/run/log/kmxa.log`	Registra actividades relacionadas con el servicio de cliente en el host de confianza ESXi.
Servicio de proveedor de claves	`/var/run/log/kmxd.log`	Registra actividades relacionadas con el servicio de proveedor de claves de vSphere Trust Authority.
Servicio de atestación	`/var/run/log/attestd.log`	Registra actividades relacionadas con el servicio de atestación de vSphere Trust Authority.

Tabla 3-11. Ubicaciones de archivos de registro de ESXi (continuación)

Componente	Ubicación	Propósito
Servicio de token de ESX	/var/run/log/esxtokend.log	Registra actividades relacionadas con el servicio de token de ESX de vSphere Trust Authority.
Reenviador de API de ESX	/var/run/log/esxapiadapter.log	Registra actividades relacionadas con el reenviador de API de vSphere Trust Authority.

Proteger tráfico de registro de Fault Tolerance

VMware Fault Tolerance (FT) captura las entradas y los eventos que se producen en una máquina virtual principal y los envía a la máquina virtual secundaria, que se ejecuta en otro host.

Este tráfico de registro entre la máquina virtual principal y la secundaria está descifrado y contiene datos de la red invitada y de la E/S de almacenamiento, así como también contenido de memoria del sistema operativo invitado. Este tráfico puede incluir datos confidenciales como contraseñas en texto sin formato. Para evitar que estos datos se divulguen, asegúrese de que la red esté protegida, especialmente contra ataques de intermediarios ("Man in the middle"). Por ejemplo, use una red privada para el tráfico de registro de FT. También puede cifrar el tráfico de registro de FT.

Activar el cifrado de Fault Tolerance

Puede cifrar el tráfico de registro de Fault Tolerance.

vSphere Fault Tolerance realiza comprobaciones frecuentes entre una máquina virtual principal y una máquina virtual secundaria, de modo que la máquina virtual secundaria se pueda reanudar rápidamente desde el último punto de control correcto. El punto de control contiene el estado de la máquina virtual que se modificó desde el punto de control anterior. Puede cifrar el tráfico de registro de Fault Tolerance.

Cuando se activa Fault Tolerance, el cifrado de FT se establece en **Oportunista** de forma predeterminada, lo que significa que activa el cifrado solo si el host principal y el secundario son capaces de cifrar. Siga este procedimiento si necesita cambiar manualmente el modo de cifrado de FT.

Nota Fault Tolerance admite el cifrado de máquinas virtuales de vSphere con vSphere 7.0 Update 2 y versiones posteriores. El cifrado en invitados y basado en matrices no depende del cifrado de máquinas virtuales ni interfiere con este. Al tener varias capas de cifrado, se utilizan recursos informáticos adicionales, lo que puede afectar al rendimiento de las máquinas virtuales. El impacto varía según el hardware, así como la cantidad y el tipo de E/S, pero el impacto general es insignificante para la mayoría de las cargas de trabajo. La eficacia y la compatibilidad de las funciones de almacenamiento back-end, como la desduplicación, la compresión y la replicación, también pueden verse afectadas por el cifrado de máquinas virtuales.

Requisitos previos

El cifrado de FT requiere SMP-FT. No se admite el cifrado en FT heredado (FT de grabación/reproducción).

Procedimiento

1 Seleccione la máquina virtual y seleccione **Editar configuración**.

2 En **Opciones de máquina virtual**, seleccione el menú despegable **FT cifrado**.

3 Seleccione una de las siguientes opciones:

Opción	Descripción
Deshabilitado	No active el registro de Fault Tolerance cifrado.
Oportunista	Active el cifrado solo si ambos lados son capaces. Una máquina virtual con Fault Tolerance puede moverse a un host ESXi que no admite el registro cifrado de Fault Tolerance.
Obligatorio	Elija hosts para Fault Tolerance principal y secundario que admitan el registro de FT cifrado.

Nota Mientras el cifrado de máquina virtual está activado, el modo de cifrado de FT se establece en **Requerido** de forma predeterminada y no se puede modificar.

Cuando el modo de cifrado de FT se establece **Requerido**:

- Cuando se habilita FT, solo se enumeran los hosts compatibles con cifrado de FT para la colocación de FT secundario.
- La conmutación por error de FT solo puede suceder en los hosts compatibles con cifrado de FT.

4 Haga clic en **Aceptar**.

Administrar registros de auditoría de ESXi

Los registros de auditoría cumplen con RFC 5424 y contienen información sobre eventos relacionados con elementos como la hora, el estado, la descripción y la información del usuario que se ha registrado para los eventos que se han producido a partir de acciones en hosts ESXi. El mantenimiento de registros de auditoría locales y remotos está disponible. El mantenimiento de registros de auditoría está desactivado de forma predeterminada. Tiene que activar manualmente los modos de auditoría local y remoto.

El registro de auditoría de ESXi local funciona como un búfer de tamaño fijo de los mensajes de auditoría recientes. Una vez que los mensajes llenan el búfer, los registros nuevos sobrescriben los registros más antiguos. El registro de auditoría remoto reenvía la misma secuencia de registros de auditoría en un formato de syslog estándar (RFC 3164) a un servidor remoto, ya sea en formato sin cifrar o cifrado (RFC 5425). Los mensajes de auditoría cumplen con RFC 5424, pero los mensajes de syslog generales solo cumplen con RFC 3164. El sistema envía un mensaje de auditoría generado al almacén local y al almacén remoto de forma simultánea.

Durante una pérdida de conexión entre el host y el almacén remoto, el almacén remoto descarta los mensajes de auditoría generados. Tras la reconexión, el sistema genera un mensaje de auditoría que indica una posible pérdida de mensajes.

Configurar registros de auditoría

Utilice ESXCLI para configurar el mantenimiento de registros de auditoría local. Para obtener más información, consulte *Conceptos y ejemplos de ESXCLI*.

Ver registros de auditoría

Puede ver los registros de auditoría de la siguiente manera.

- Local: utilice la aplicación ESXi `/bin/viewAudit`.
- Remoto: configure un servidor de auditoría remoto mediante ESXCLI. Para obtener más información, consulte Habilitar la transmisión de registros de auditoría a un host remoto con ESXCLI.

También puede utilizar la API FetchAuditRecords (en el objeto administrado DiagnosticsManager) para ver los registros de auditoría.

Cómo asegurar la configuración de ESXi

En vSphere 7.0 Update 2 y versiones posteriores, la configuración de ESXi está protegida mediante el cifrado.

Qué es una configuración de ESXi segura

Muchos servicios ESXi guardan secretos en sus archivos de configuración. Estas configuraciones se conservan en un banco de arranque del host ESXi como un archivo archivado. Antes de vSphere 7.0 Update 2, el archivo de configuración ESXi archivado no está cifrado. En vSphere 7.0 Update 2 y versiones posteriores, se cifra el archivo de configuración archivado. Como resultado, los atacantes no pueden leer ni alterar este archivo directamente, incluso si tienen acceso físico al almacenamiento del host ESXi.

Además de evitar que un atacante acceda a secretos, una configuración segura de ESXi cuando se utiliza con un TPM puede guardar claves de cifrado de máquinas virtuales después de reiniciar. Cuando el host ESXi está configurado con un TPM, el TPM se utiliza para "sellar" la configuración en el host, lo que proporciona una garantía de seguridad sólida. Como resultado, las cargas de trabajo cifradas pueden seguir funcionando cuando un servidor de claves no está disponible o no se puede acceder a él. Consulte Persistencia de claves de vSphere en hosts ESXi.

No es necesario activar el cifrado de la configuración de ESXi manualmente. Cuando instala o actualiza a vSphere 7.0 Update 2 o posterior, se cifra el archivo de configuración ESXi archivado.

Para las tareas asociadas con una configuración de ESXi segura, consulte Administrar una configuración de ESXi segura.

Archivos de configuración de ESXi anteriores a vSphere 7.0 Update 2

La configuración de un host ESXi consta de archivos de configuración para cada servicio que se ejecuta en el host. Los archivos de configuración suelen residir en el directorio `/etc/`, pero también pueden residir en otros espacios de nombres. Los archivos de configuración contienen información en tiempo de ejecución sobre el estado de los servicios. Con el tiempo, los valores predeterminados de los archivos de configuración pueden cambiar, por ejemplo, cuando se cambia la configuración en el host ESXi. Un trabajo cron realiza una copia de seguridad de los archivos de configuración de ESXi periódicamente, o cuando ESXi se apaga correctamente o a pedido, y crea un archivo de configuración archivado en el banco de arranque. Cuando ESXi se reinicia, lee el archivo de configuración archivado y vuelve a crear el estado en el que ESXi estaba cuando se creó la copia de seguridad. Antes de vSphere 7.0 Update 2, el archivo de configuración archivado no está cifrado. Como resultado, es posible que un atacante que tenga acceso al almacenamiento de ESXi físico lea y altere este archivo mientras el sistema está sin conexión.

Cómo se implementa una configuración de ESXi segura

Durante el primer arranque después de instalar o actualizar el host ESXi a vSphere 7.0 Update 2 o posterior, ocurre lo siguiente:

- Si el host ESXi tiene un TPM y está activado en el firmware, el archivo de configuración archivado se cifra mediante una clave de cifrado almacenada en el TPM. A partir de este punto, la configuración del host está sellada por el TPM.
- Si el host ESXi no tiene un TPM, ESXi utiliza una función de derivación de claves (KDF) para generar una clave de cifrado de configuración segura para el archivo de configuración archivado. Las entradas al archivo KDF se almacenan en el disco en el archivo `encryption.info`.

Nota Cuando un host ESXi tiene un dispositivo TPM activado, se obtiene protección adicional.

Cuando el host ESXi se reinicia después del primer arranque, ocurre lo siguiente:

- Si el host ESXi tiene un TPM, el host debe obtener la clave de cifrado del TPM para ese host específico. Si las mediciones de TPM cumplen la directiva de sellado que se utilizó al crear la clave de cifrado, el host obtiene la clave de cifrado del TPM.
- Si el host ESXi no tiene un TPM, ESXi lee la información del archivo `encryption.info` para desbloquear la configuración segura.

Requisitos de configuración ESXi segura

- ESXi 7.0 Update 2 o una versión posterior
- TPM 2.0 para el cifrado de configuración y la capacidad de usar una directiva de sellado

Clave de recuperación de la configuración de ESXi segura

Una configuración de ESXi segura incluye una clave de recuperación. Si debe recuperar la configuración de ESXi segura, utilice una clave de recuperación cuyo contenido introduzca como opción de arranque de línea de comandos. Puede enumerar la clave de recuperación para crear una copia de seguridad de la clave de recuperación. También puede rotar la clave de recuperación como parte de los requisitos de seguridad.

Realizar una copia de seguridad de la clave de recuperación es una parte importante de la administración de la configuración de ESXi segura. vCenter Server genera una alarma para recordarle que cree una copia de seguridad de la clave de recuperación.

Alarma de la clave de recuperación de la configuración de ESXi segura

Realizar una copia de seguridad de la clave de recuperación es una parte importante de la administración de la configuración de ESXi segura. Cada vez que un host de ESXi en modo TPM se conecta o se vuelve a conectar a vCenter Server, vCenter Server genera una alarma para recordarle que haga una copia de seguridad de la clave de recuperación. Cuando se restablece la alarma, no se vuelve a activar a menos que las condiciones cambien.

Prácticas recomendadas para la configuración de ESXi segura

Siga estas prácticas recomendadas para la clave de recuperación de ESXi segura:

- Cuando se enumera una clave de recuperación, esta se muestra temporalmente en un entorno que no es de confianza y se encuentra en la memoria. Quite los rastros de la clave.
  - Al reiniciar el host, se elimina la clave residual de la memoria.
  - Para mejorar la protección, puede activar el modo de cifrado en el host. Consulte Activar el modo de cifrado de host de forma explícita.
- Al realizar una recuperación:
  - Para eliminar cualquier rastreo de la clave de recuperación en un entorno que no sea de confianza, reinicie el host.
  - Para mejorar la seguridad, rote la clave de recuperación para utilizar una nueva clave después de haber recuperado la clave una vez.

Qué son las directivas de sellado de TPM

Un TPM puede utilizar las mediciones del registro de configuración de la plataforma (Platform Configuration Register, PCR) para implementar directivas que restrinjan el acceso no autorizado a los datos confidenciales. Cuando instala vSphere 7.0 Update 2 y versiones posteriores en un host ESXi con un TPM o actualiza el host a dicha versión, el TPM sella la información

confidencial mediante una directiva que incorpora la configuración de arranque seguro. Esta directiva comprueba que, si el arranque seguro se activó cuando los datos se sellaron por primera vez con el TPM, este siga estando activado cuando se intente quitar el sello de los datos en un arranque posterior.

El arranque seguro forma parte del estándar de firmware UEFI. Con el arranque seguro UEFI activado, un host se niega a cargar cualquier aplicación o controlador UEFI, salvo que el cargador de arranque del sistema operativo tenga una firma digital válida.

Puede desactivar o activar la aplicación del arranque seguro UEFI. Consulte Activar o desactivar la aplicación del arranque seguro para una configuración de ESXi segura.

Nota Si no activa un TPM al instalar o actualizar a vSphere 7.0 Update 2 o una versión posterior, puede hacerlo más tarde con el siguiente comando.

```
esxcli system settings encryption set --mode=TPM
```

Una vez que haya activado el TPM, no podrá deshacer la configuración.

Se produce un error en el comando `esxcli system settings encryption set` en algunos TPM, incluso cuando el TPM está activado para el host.

- En vSphere 7.0 Update 2: TPM de NationZ (NTZ), Infineon Technologies (IFX) y ciertos modelos nuevos (como NPCT75x) de Nuvoton Technologies Corporation (NTC)
- En vSphere 7.0 Update 3: TPM de NationZ (NTZ)

Si una instalación o actualización de vSphere 7.0 Update 2 o una versión posterior no puede utilizar el TPM durante el primer arranque, la instalación o la actualización continúan y el modo predeterminado es NINGUNO (es decir, `--mode=NONE`). El comportamiento resultante es como si el TPM no estuviera activado.

El TPM también puede aplicar la configuración para la opción de arranque execInstalledOnly en la directiva de sellado. La aplicación de execInstalledOnly es una opción avanzada de arranque de ESXi que garantiza que el Vmkernel ejecute solo archivos binarios que se empaquetaron y firmaron correctamente como parte de un VIB. La opción de arranque execInstalledOnly depende de la opción de arranque seguro. La aplicación del arranque seguro debe estar activada para poder aplicar la opción de arranque execInstalledOnly en la directiva de sellado. Consulte Activar o desactivar la aplicación execInstalledOnly para una configuración de ESXi segura.

Administrar una configuración de ESXi segura

Puede usar comandos ESXCLI para enumerar la clave de recuperación de la configuración de ESXi segura, rotar la clave de recuperación y cambiar las directivas de TPM (por ejemplo, aplicar el arranque seguro UEFI).

Mostrar el contenido de la clave de recuperación de configuración de ESXi seguridad

Puede utilizar ESXCLI para mostrar el contenido de la clave de recuperación de configuración ESXi de seguridad.

Esta tarea se aplica solo a un host ESXi que tiene un TPM. En general, puede enumerar el contenido de la clave de recuperación de configuración ESXi segura para crear una copia de seguridad o como parte de la rotación de claves de recuperación.

Requisitos previos

- Tener acceso al conjunto de comandos de ESXCLI. Puede ejecutar comandos ESXCLI de forma remota o en ESXi Shell.
- Privilegio necesario para usar la versión independiente de ESXCLI o PowerCLI: **Host.Config.Settings**

Procedimiento

1 Ejecute el siguiente comando en el host ESXi.

```
esxcli system settings encryption recovery list
```

2 Guarde la salida en una ubicación remota y segura como copia de seguridad en caso de que deba recuperar la configuración segura.

Resultados

Se muestran el identificador y la clave de la clave de recuperación.

Ejemplo: Enumerar la clave de recuperación de configuración de ESXi secura

```
[root@host1] esxcli system settings encryption recovery list

Recovery ID                              Key
-------------------------------------    ---
{2DDD5424-7F3F-406A-8DA8-D62630F6C8BC}
478269-039194-473926-430939-686855-231401-642208-184477-602511
-225586-551660-586542-338394-092578-687140-267425
```

Rotar la clave de recuperación de configuración de ESXi segura

Puede usar ESXCLI para rotar la clave de recuperación de configuración de ESXi.

Esta tarea se aplica solo a un host ESXi que tiene un TPM. Es posible rotar la clave de recuperación de configuración de ESXi segura como parte de las prácticas recomendadas de seguridad.

Requisitos previos

- Tener acceso al conjunto de comandos de ESXCLI. Puede ejecutar comandos ESXCLI de forma remota o en ESXi Shell.

- Privilegio necesario para usar la versión independiente de ESXCLI o PowerCLI: **Host.Config.Settings**

Procedimiento

1. Enumere la clave de recuperación.

   Consulte Mostrar el contenido de la clave de recuperación de configuración de ESXi seguridad.

2. Ejecute el siguiente comando.

   ```
   esxcli system settings encryption recovery rotate [-k keyID] -u uuid
   ```

   En este comando, el *keyID* opcional es el identificador de clave en la memoria caché de claves de VMkernel y *uuid* es el identificador de recuperación (obtenido del comando `esxcli system settings encryption recovery list`). Si no proporciona el identificador de clave opcional, ESXi reemplaza la clave de recuperación anterior por una nueva clave de recuperación que se genera de forma aleatoria.

Resultados

La clave de recuperación ahora está configurada con el contenido de la clave a la que hace referencia el identificador de clave, si se proporciona. De lo contrario, ESXi proporciona un nuevo identificador de clave.

Solución y recuperación de problemas de la configuración segura de ESXi

Puede solucionar y recuperarse de los problemas de arranque que podría encontrar con una configuración segura de ESXi.

Si se borra un TPM (es decir, se restablecen los valores de inicialización del TPM) o si se produce un error en un TPM o si se reemplaza la placa base o el dispositivo de TPM, debe realizar los pasos necesarios para recuperar la configuración segura de ESXi. Debe tener la clave de recuperación para recuperar la configuración. Hasta que no se recupere la configuración, el host ESXi no puede arrancar. Consulte Recuperar la configuración de ESXi segura.

Aunque es poco común, es posible que un host ESXi no pueda restaurar o descifrar la configuración segura, lo que impide que el host arranque. Las posibles situaciones incluyen:

- Cambio a la configuración de arranque seguro (u otra directiva)
- Manipulación real
- La clave de recuperación no está disponible

Para solucionar estos problemas, consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/81446

Recuperar la configuración de ESXi segura

Si se produce un error en un TPM o si borra un TPM, debe recuperar la configuración de ESXi segura. Hasta que no se recupere la configuración, el host ESXi no puede arrancar.

La recuperación de la configuración ESXi segura hace referencia a las siguientes situaciones:

- Ha borrado el TPM (es decir, se han restablecido las inicializaciones del TPM).
- Se produjo un error del TPM.
- Reemplazó la placa base o el dispositivo TPM, o ambos.

Para solucionar otros problemas de configuración de ESXi segura, consulte el artículo VMware la base de conocimientos en https://kb.vmware.com/s/article/81446.

Realice la recuperación manualmente. No realice la recuperación como parte de un script de instalación o actualización.

Requisitos previos

Obtenga la clave de recuperación. Debería haber enumerado y almacenado previamente la clave de recuperación. Consulte Mostrar el contenido de la clave de recuperación de configuración de ESXi seguridad.

Procedimiento

1 (opcional) Si ha fallado el TPM, mueva el disco (con el banco de arranque) a otro host con un TPM.

2 Inicie el host ESXi.

3 Cuando aparezca la ventana del instalador de ESXi, presione las teclas Mayús + O para editar las opciones de arranque.

4 Para recuperar la configuración en el símbolo del sistema, anexe la siguiente opción de arranque a cualquier opción de arranque existente.

```
encryptionRecoveryKey=recovery_key
```

La configuración de ESXi segura se recupera y el host ESXi arranca.

5 Para conservar el cambio, introduzca el siguiente comando:

```
/sbin/auto-backup.sh
```

Pasos siguientes

Al introducir la clave de recuperación, esta se muestra temporalmente en un entorno que no es de confianza y se encuentra en la memoria. Aunque no es necesario, como práctica recomendada, puede eliminar los rastros residuales de la clave en la memoria reiniciando el host. O bien, puede girar la clave. Consulte Rotar la clave de recuperación de configuración de ESXi segura.

Activar o desactivar la aplicación del arranque seguro para una configuración de ESXi segura

Puede optar por activar la aplicación de arranque seguro UEFI o desactivar una aplicación de arranque seguro UEFI previamente activada. Debe utilizar ESXCLI para cambiar la configuración del TPM en el ESXi host.

Esta tarea se aplica solo a ESXi hosts que tienen un TPM. El arranque seguro UEFI es una configuración de firmware para garantizar que el software iniciado por el firmware sea de confianza. Para obtener más información, consulte Arranque seguro UEFI para hosts ESXi. La habilitación del arranque seguro UEFI se puede aplicar en cada arranque mediante TPM.

Requisitos previos

- Tener acceso al conjunto de comandos de ESXCLI. Puede ejecutar comandos ESXCLI de forma remota o en ESXi Shell.
- Privilegio necesario para usar la versión independiente de ESXCLI o PowerCLI: **Host.Config.Settings**

Procedimiento

1 Enumere la configuración actual del ESXi host.

```
esxcli system settings encryption get
   Mode: TPM
   Require Executables Only From Installed VIBs: false
   Require Secure Boot: true
```

Si la aplicación del arranque seguro está activada, la opción Requerir arranque seguro (Require Secure Boot) muestra el valor true (cierto). Si la aplicación del arranque seguro está desactivada, la opción Requerir arranque seguro (Require Secure Boot) muestra el valor false (falso).

Si Modo aparece como NINGUNO, debe activar el TPM en el firmware y establecer el modo mediante el siguiente comando:

```
esxcli system settings encryption set --mode=TPM
```

2 Active o desactive la aplicación del arranque seguro.

<table>
<tr><th>Opción</th><th>Descripción</th></tr>
<tr><td>Activar</td><td>
a Apague el host correctamente.
Por ejemplo, haga clic con el botón secundario en ESXi host en el vSphere Client y seleccione Power > Shut Down.
b Active el arranque seguro en el firmware del host.
Consulte la documentación de hardware de su proveedor específico.
c Reinicie el host.
d Ejecute el siguiente comando ESXCLI.
<pre>esxcli system settings encryption set --require-secure-
boot=T</pre>
e Verifique el cambio.
<pre>esxcli system settings encryption get
   Mode: TPM
   Require Executables Only From Installed VIBs: false
   Require Secure Boot: true</pre>
Confirme que el valor de Arranque seguro requerido (Required Secure Boot) se muestre en true (cierto).
f Para guardar la configuración, ejecute el siguiente comando:
<pre>/bin/backup.sh 0</pre>
</td></tr>
<tr><td>Desactivar</td><td>
a Ejecute el siguiente comando ESXCLI.
<pre>esxcli system settings encryption set --require-secure-
boot=F</pre>
b Verifique el cambio.
<pre>esxcli system settings encryption get
   Mode: TPM
   Require Executables Only From Installed VIBs: false
   Require Secure Boot: false</pre>
Confirme que Requerir arranque seguro (Require Secure Boot) muestre el valor false (falso).
c Para guardar la configuración, ejecute el siguiente comando:
<pre>/bin/backup.sh 0</pre>
Puede optar por desactivar el arranque seguro en el firmware del host, pero en este punto ya no se establece la dependencia entre la configuración de firmware y la aplicación de TPM.
</td></tr>
</table>

Resultados

El host ESXi se ejecuta con la aplicación de arranque seguro activada o desactivada, según cuál sea su elección.

Nota Si no activa un TPM al instalar o actualizar a vSphere 7.0 Update 2 o una versión posterior, puede hacerlo más tarde con el siguiente comando.

```
esxcli system settings encryption set --mode=TPM
```

Una vez que haya activado el TPM, no podrá deshacer la configuración.

Se produce un error en el comando `esxcli system settings encryption set` en algunos TPM, incluso cuando el TPM está activado para el host.

- En vSphere 7.0 Update 2: TPM de NationZ (NTZ), Infineon Technologies (IFX) y ciertos modelos nuevos (como NPCT75x) de Nuvoton Technologies Corporation (NTC)
- En vSphere 7.0 Update 3: TPM de NationZ (NTZ)

Si una instalación o actualización de vSphere 7.0 Update 2 o una versión posterior no puede utilizar el TPM durante el primer arranque, la instalación o la actualización continúan y el modo predeterminado es NINGUNO (es decir, `--mode=NONE`). El comportamiento resultante es como si el TPM no estuviera activado.

Activar o desactivar la aplicación execInstalledOnly para una configuración de ESXi segura

Puede activar la aplicación execInstalledOnly o desactivar una aplicación execInstalledOnly habilitada previamente. Debe utilizar ESXCLI para cambiar la configuración del TPM en el ESXi host. La aplicación del arranque seguro UEFI debe estar activada antes de poder activar la aplicación execInstalledOnly.

Esta tarea se aplica solo a ESXi hosts que tienen un TPM. La opción de arranque ESXi execInstalledOnly, cuando se establece en TRUE, garantiza que el VMkernel ejecute solo los archivos binarios que se empaquetaron y firmaron como parte de un VIB. La habilitación de esta opción de arranque se puede aplicar en cada arranque mediante el uso de TPM.

Requisitos previos

- Para activar la aplicación execInstalledOnly, primero debe activar la aplicación de arranque seguro UEFI. La aplicación execInstalledOnly está integrada en la aplicación de arranque seguro UEFI. Consulte Activar o desactivar la aplicación del arranque seguro para una configuración de ESXi segura.
- Tener acceso al conjunto de comandos de ESXCLI. Puede ejecutar comandos ESXCLI de forma remota o en ESXi Shell.
- Privilegio necesario para usar la versión independiente de ESXCLI o PowerCLI: **Host.Config.Settings**

Procedimiento

1 Enumere la configuración actual del ESXi host.

```
esxcli system settings encryption get
   Mode: TPM
   Require Executables Only From Installed VIBs: false
   Require Secure Boot: true
```

Si la aplicación execInstalledOnly está activada, la opción Requerir ejecutables solo desde los VIB instalados (Require Executables Only From Installed VIBs) muestra el valor true (cierto). Si la aplicación execInstalledOnly está desactivada, la opción Requerir ejecutables solo desde los VIB instalados (Require Executables Only From Installed VIBs) muestra el valor false (falso). Para activar la aplicación execInstalledOnly, la aplicación de arranque seguro debe estar activada y Requerir arranque seguro (Require Secure Boot) muestra el valor true (cierto) en este caso.

Si Modo aparece como NINGUNO, debe habilitar el TPM en el firmware y establecer el modo mediante el siguiente comando:

```
esxcli system settings encryption set --mode=TPM
```

Además, si Requerir arranque seguro (Require Secure Boot) aparece como False, consulte Activar o desactivar la aplicación del arranque seguro para una configuración de ESXi segura si desea activar esa exigencia.

2 Active o desactive la aplicación execInstalledOnly.

Opción	Descripción
Activar	a Compruebe que la opción de arranque seguro esté activada. `esxcli system settings encryption get` `   Mode: TPM` `   Require Executables Only From Installed VIBs: false` `   Require Secure Boot: true` Confirme que la opción Requerir arranque seguro (Require Secure Boot) se muestre en true. Si no es así, consulte Activar o desactivar la aplicación del arranque seguro para una configuración de ESXi segura. b Para configurar el valor de tiempo de ejecución de la opción de arranque execInstalledOnly en TRUE, ejecute el siguiente comando ESXCLI. `esxcli system settings kernel set -s execInstalledOnly -v TRUE` c Apague el host correctamente. Por ejemplo, haga clic con el botón secundario en ESXi host en el vSphere Client y seleccione **Power > Shut Down**. d Reinicie el host. e Para establecer la aplicación execInstalledOnly, ejecute el siguiente comando ESXCLI. `esxcli system settings encryption set --require-exec-installed-only=T` f Verifique el cambio. `esxcli system settings encryption get` `   Mode: TPM` `   Require Executables Only From Installed VIBs: true` `   Require Secure Boot: true` Confirme que la opción Requerir ejecutables solo desde los VIB instalados (Require Executables Only From Installed VIB) muestre el valor true. g Para guardar la configuración, ejecute el siguiente comando: `/bin/backup.sh 0`
Desactivar	a Ejecute el siguiente comando ESXCLI. `esxcli system settings encryption set --require-exec-installed-only=F` b Verifique el cambio. `esxcli system settings encryption get` `   Mode: TPM` `   Require Executables Only From Installed VIBs: false` `   Require Secure Boot: true` Confirme que la opción Requerir ejecutables solo desde los VIB instalados muestre el valor false.

Opción	Descripción
	c Para guardar la configuración, ejecute el siguiente comando: `/bin/backup.sh 0` El TPM ya no aplica la opción de arranque execInstalledOnly.

Resultados

El host ESXi se ejecuta con la aplicación execInstalledOnly activada o desactivada, según cuál sea su elección.

Desactivar la opción interna de tiempo de ejecución de execInstalledOnly

Cuando actualiza a ESXi 8.0 o una versión posterior, o bien la instala, la opción interna de tiempo de ejecución de execInstalledOnly se activa en los hosts de forma predeterminada. Esta opción ayuda a proteger los hosts contra ataques de ransomware. Si los hosts ESXi 8.0 o una versión posterior siguen ejecutando archivos binarios que no son de VIB de orígenes externos, puede desactivar la opción interna de tiempo de ejecución de execInstalledOnly.

Con la opción execInstalledOnly se protegen los hosts contra ataques de ransomware, ya que se garantiza que el VMkernel ejecute solo esos archivos binarios en un host y que se hayan empaquetado y firmado correctamente como parte de un VIB válido.

La opción execInstalledOnly es tanto una opción de arranque como una opción interna de tiempo de ejecución. La opción de arranque execInstalledOnly, también llamada opción de kernel, se introdujo en ESXi 5.5. La opción de arranque execInstalledOnly está desactivada de forma predeterminada. En vSphere 7.0 Update 2 o versiones posteriores, es posible aplicar la opción de arranque execInstalledOnly en cada arranque mediante un TPM. Para obtener más información, consulte Activar o desactivar la aplicación execInstalledOnly para una configuración de ESXi segura.

La opción interna de tiempo de ejecución de execInstalledOnly que se agregó en ESXi 8.0 está activada en los hosts de forma predeterminada. La opción de arranque de execInstalledOnly continúa desactivada de forma predeterminada, excepto cuando una opción de arranque execInstalledOnly que se habilitó anteriormente sobrescribe la opción interna de tiempo de ejecución si se establecen ambas opciones.

Nota La opción execInstalledOnly es independiente del arranque seguro. El arranque seguro comprueba que todos los VIB instalados estén firmados. Para obtener más información, consulte Arranque seguro UEFI para hosts ESXi.

Cuando se desactiva la opción interna de tiempo de ejecución de execInstalledOnly, se muestran advertencias de vCenter Server para el host.

Requisitos previos

Para desactivar la opción interna de tiempo de ejecución de execInstalledOnly, debe tener acceso raíz al host ESXi. Puede utilizar ESXCLI, PowerCLI o la API. La tarea que sigue utiliza ESXCLI.

Precaución Si desactiva la opción interna de tiempo de ejecución de execInstalledOnly, estará más expuesto a sufrir ataques.

Procedimiento

1 Conéctese al host ESXi mediante SSH.

2 Para desactivar la opción interna de tiempo de ejecución de execInstalledOnly, introduzca el siguiente comando ESXCLI.

```
esxcli system settings advanced set -o /User/execInstalledOnly -i 0
```

Proteger sistemas vCenter Server

4

La protección de vCenter Server incluye la seguridad del host en el que se ejecuta vCenter Server, el cumplimiento de las prácticas recomendadas para asignar privilegios y funciones, y la comprobación de la integridad de los clientes que se conectan a vCenter Server.

Lea los siguientes temas a continuación:

Prácticas recomendadas sobre el control de acceso a vCenter Server

Realice un control estricto del acceso a los diferentes componentes de vCenter Server a fin de aumentar la seguridad del sistema.

Las siguientes instrucciones ayudan a garantizar la seguridad del entorno.

Usar cuentas con nombre para acceder a vCenter Server

- Otorgue la función de administrador únicamente a aquellos administradores que la necesiten. Se pueden crear funciones personalizadas o se puede usar la función de administrador Sin criptografía para los administradores que tienen privilegios más limitados. No aplique esta función a ningún grupo cuya pertenencia no esté estrictamente controlada.
- Compruebe que las aplicaciones usen cuentas de servicio únicas al conectarse a un sistema vCenter Server.

Supervisar los privilegios de los usuarios administradores de vCenter Server

No todos los usuarios administradores deben tener la función de administrador. En cambio, se puede crear una función personalizado con el conjunto adecuado de privilegios y asignárselo a otros administradores.

Los usuarios con la función de administrador de vCenter Server tienen privilegios sobre todos los objetos de la jerarquía. Por ejemplo, la función de administrador permite, de forma predeterminada, que los usuarios interactúen con los archivos y los programas que se encuentran en el sistema operativo invitado de una máquina virtual. Si se asigna esa función a demasiados usuarios, se puede reducir la confidencialidad, la disponibilidad o la integridad de los datos de la máquina virtual. Cree una función que les otorgue a los administradores los privilegios que necesitan, pero elimine algunos de los privilegios de administración de la máquina virtual. Vea también Usar registrador de privilegios.

Minimizar el acceso a vCenter Server Appliance

No permita que los usuarios inicien sesión directamente en vCenter Server Appliance. Los usuarios cuya sesión en vCenter Server Appliance está iniciada pueden causar daños, ya sea intencionales o involuntarios, al alterar la configuración y modificar los procesos. Esos usuarios pueden llegar a acceder a las credenciales de vCenter Server, como el certificado SSL. Permita iniciar sesión en el sistema solo a los usuarios que puedan realizar tareas legítimas y asegúrese de que se auditen los eventos de inicio de sesión.

Otorgar privilegios mínimos a los usuarios de base de datos

El usuario de base de datos precisa solamente ciertos privilegios específicos para el acceso a la base de datos.

Algunos privilegios son necesarios solamente para la instalación y las actualizaciones. Estos privilegios se pueden eliminar desde el administrador de la base de datos una vez que vCenter Server se haya instalado o actualizado.

Restringir el acceso al explorador del almacén de datos

Asigne el privilegio **Almacén de datos.Examinar almacén de datos** solo a los usuarios o grupos que realmente lo necesiten. Los usuarios que tienen el privilegio pueden ver, cargar o descargar archivos en almacenes de datos asociados con la implementación de vSphere a través del explorador web o vSphere Client.

Restringir la ejecución de comandos en una máquina virtual a los usuarios

De forma predeterminada, un usuario con la función de administrador puede interactuar con los archivos y los programas de un sistema operativo invitado dentro de una máquina virtual. Para reducir el riesgo de infracciones de confidencialidad, disponibilidad o integridad del invitado, cree una función personalizada de acceso que no sea de invitado en la que no esté el privilegio **Máquina virtual.Operaciones de invitado**. Consulte Restringir la ejecución de comandos dentro de una máquina virtual a los usuarios.

Considerar la modificación de la directiva de contraseñas para vpxuser

De manera predeterminada, vCenter Server cambia la contraseña de vpxuser automáticamente cada 30 días. Asegúrese de que esta configuración respete la directiva de la empresa o configure la directiva de contraseñas de vCenter Server. Consulte Configurar la directiva de contraseñas de vCenter Server.

Nota Compruebe que la directiva de caducidad de contraseñas no sea demasiado corta.

Comprobar privilegios después de reiniciar vCenter Server

Revise la reasignación de privilegios al reiniciar vCenter Server. Si el usuario o el grupo que tienen la función de administrador en la carpeta raíz no se pueden validar durante el reinicio, la función se elimina de ese usuario o grupo. En su lugar, vCenter Server otorga la función de administrador al administrador de vCenter Single Sign-On, administrator@vsphere.local de forma predeterminada. De ese modo, esta cuenta puede actuar como administrador de vCenter Server.

Restablezca la cuenta de administrador con nombre y asigne la función de administrador a dicha cuenta para evitar usar la cuenta de administrador anónima de vCenter Single Sign-On (de manera predeterminada, administrator@vsphere.local).

Usar niveles altos de cifrado para el protocolo de escritorio remoto

Asegúrese de que en cada equipo con Windows de la infraestructura se establezca una configuración de host del protocolo de escritorio remoto (Remote Desktop Protocol, RDP) a fin de garantizar el nivel más alto de cifrado adecuado para el entorno.

Comprobar certificados de vSphere Client

Indique a los usuarios de vSphere Client o de otras aplicaciones cliente que pongan atención a las advertencias de comprobación de certificados. Sin la comprobación de certificados, el usuario puede ser víctima de un ataque de MiTM.

Configurar la directiva de contraseñas de vCenter Server

De manera predeterminada, vCenter Server cambia la contraseña de vpxuser automáticamente cada 30 días. Puede cambiar este valor desde vSphere Client.

Procedimiento

1 Inicie sesión en el sistema vCenter Server mediante vSphere Client.

2 Seleccione el sistema de vCenter Server en la jerarquía de objetos.

3 Haga clic en **Configurar**.

4 Haga clic en **Configuración avanzada** y en **Editar configuración**.

5 Haga clic en el icono **Filtrar** e introduzca **`VimPasswordExpirationInDays`**.

6 Configure `VirtualCenter.VimPasswordExpirationInDays` para que cumpla con sus requisitos.

Quitar certificados caducados o revocados, y registros de instalaciones con errores

Dejar certificados caducados o revocados, o dejar registros de instalación incorrecta de vCenter Server en el sistema vCenter Server puede perjudicar el entorno.

Los certificados caducados o revocados deben eliminarse por los siguientes motivos.

- Si los certificados caducados o revocados no se eliminan del sistema vCenter Server, el entorno puede quedar vulnerable a un ataque de MiTM.
- En ciertos casos, si la instalación de vCenter Server no se realiza correctamente, se crea en el sistema un archivo de registro que contiene la contraseña de la base de datos en texto sin formato. Un atacante que logre entrar al sistema vCenter Server puede tener acceso a esta contraseña y, al mismo tiempo, acceder a la base de datos de vCenter Server.

Limitar la conectividad de red de vCenter Server

Para mejorar la seguridad, evite colocar el sistema vCenter Server en otra red distinta de la red de administración, y asegúrese de que el tráfico de administración de vSphere se encuentre en una red restringida. Al limitar la conectividad de red, se limitan ciertos tipos de ataques.

vCenter Server requiere acceso solamente a una red de administración. Evite colocar el sistema vCenter Server en otras redes, como la red de producción o la de almacenamiento, o en otra red con acceso a Internet. vCenter Server no necesita acceder a la red donde funciona vMotion.

vCenter Server requiere conectividad de red con los siguientes sistemas.

- Todos los hosts ESXi.
- La base de datos de vCenter Server.
- Otros sistemas de vCenter Server (si los sistemas de vCenter Server forman parte de un dominio de vCenter Single Sign-On común con fines de replicación de etiquetas, permisos, etc.).

- Los sistemas que están autorizados para ejecutar clientes de administración. Por ejemplo, vSphere Client, un sistema Windows donde se utiliza PowerCLI o cualquier otro cliente basado en SDK.
- Los servicios de infraestructura como DNS, Active Directory y NTP.
- Otros sistemas que ejecutan componentes fundamentales para la funcionalidad del sistema vCenter Server.

Utilice el firewall en la instancia de vCenter Server. Incluya restricciones de acceso basadas en IP de modo que solo los componentes necesarios puedan comunicarse con el sistema vCenter Server.

Evaluación del uso de clientes Linux con CLI y SDK

Las comunicaciones entre los componentes del cliente y el sistema vCenter Server o los hosts ESXi están protegidas por un cifrado basado en SSL de forma predeterminada. Las versiones de Linux de estos componentes no realizan la validación de certificados. Considere restringir el uso de estos clientes.

Para mejorar la seguridad, puede reemplazar los certificados firmados por VMCA del sistema de vCenter Server y los hosts ESXi por certificados firmados por una entidad de certificación de la empresa o de terceros. Sin embargo, ciertas comunicaciones con clientes Linux seguirán siendo vulnerables a ataques machine-in-the-middle. Los siguientes componentes son vulnerables cuando se ejecutan en el sistema operativo Linux.

- Comandos ESXCLI
- Scripts de vSphere SDK for Perl
- Programas escritos con el vSphere Web Services SDK

Si aplica los controles correspondientes, puede reducir la restricción contra el uso de clientes Linux.

- Restrinja el acceso a la red de administración únicamente a los sistemas autorizados.
- Utilice firewalls para garantizar que únicamente los hosts autorizados tengan permiso para acceder a vCenter Server.
- Utilice hosts bastión (sistemas JumpBox) para garantizar que los clientes Linux sean supervisados.

Examinar los complementos de vSphere Client

Las extensiones de vSphere Client se ejecutan en el mismo nivel de privilegio que el usuario que inició sesión. Una extensión maliciosa puede enmascararse como si fuera un complemento útil y realizar operaciones dañinas, como el robo de credenciales o cambios en la configuración del sistema. Para aumentar la seguridad, utilice una instalación en la que se incluyan únicamente extensiones autorizadas de orígenes confiables.

Una instalación de vCenter Server incluye un marco de extensibilidad para vSphere Client. Este marco se puede usar para extender el cliente con selecciones de menú o iconos de la barra de herramientas. Las extensiones pueden proporcionar acceso a los componentes complementarios de vCenter Server o la funcionalidad externa basada en web.

Al utilizar el marco de extensibilidad, se entraña el riesgo de introducir funcionalidades no intencionadas. Por ejemplo, si un administrador instala un complemento en una instancia de vSphere Client, el complemento puede ejecutar comandos arbitrarios con el nivel de privilegio de ese administrador.

Para evitar una posible transigencia de su vSphere Client, examine periódicamente todos los complementos instalados y compruebe que provienen de un origen de confianza.

Requisitos previos

Debe tener los privilegios necesarios para acceder al servicio vCenter Single Sign-On. Estos privilegios difieren de los de vCenter Server.

Procedimiento

1 Inicie sesión en vSphere Client como administrator@vsphere.local o como usuario con privilegios de vCenter Single Sign-On.

2 En la página de inicio, seleccione **Administración** y, a continuación, seleccione **Complementos del cliente** en **Soluciones**.

3 Examine la lista de complementos del cliente.

Prácticas recomendadas de seguridad de vCenter Server

Siga todas las prácticas recomendadas para proteger un sistema vCenter Server. Se proporcionan pasos adicionales a modo de ayuda para aumentar la seguridad de vCenter Server.

Configurar el protocolo de hora de precisión o el protocolo de hora de red

Asegúrese de que todos los sistemas utilicen el mismo origen de hora relativo. Este origen de hora debe estar sincronizado con un estándar de hora acordado, como la hora universal coordinada (Coordinated Universal Time, UTC). Es fundamental que los sistemas estén sincronizados para la validación de certificados. El protocolo de hora de precisión (Precision Time Protocol, PTP) y el protocolo de hora de redes (Network Time Protocol, NTP) también facilitan el seguimiento de un intruso en los archivos de registro. Una configuración de hora incorrecta dificulta la inspección y la correlación de los archivos de registro para detectar ataques, además de hacer imprecisas las auditorías. Consulte Sincronizar la hora de vCenter Server con un servidor NTP.

Restringir el acceso a la red de vCenter Server

Restrinja el acceso a los componentes que se necesiten para comunicarse con vCenter Server. Al bloquear el acceso desde sistemas innecesarios, se reducen las posibilidades de que el sistema operativo reciba ataques.

Para obtener la lista de todos los puertos y protocolos compatibles en los productos de VMware, incluidos vSphere y vSAN, consulte la herramienta VMware Ports and Protocols™ en https://ports.vmware.com/. Puede buscar puertos por producto de VMware, crear una lista de puertos personalizada e imprimir o guardar listas de puertos.

Configurar un host bastión

Para ayudar a proteger los activos, configure un host bastión (también denominado Jump Box) para realizar tareas administrativas con privilegios elevados. Un host bastión es un equipo con un propósito especial que aloja una cantidad mínima de aplicaciones administrativas. Se eliminan todos los demás servicios innecesarios. El host suele residir en la red de administración. Un host bastión aumenta la protección de los activos mediante la restricción del inicio de sesión a los individuos clave, la solicitud de reglas de firewall para iniciar sesión y la adición de supervisión mediante herramientas de auditoría.

Requisitos de contraseñas y comportamiento de bloqueo de vCenter

Para administrar el entorno de vSphere, debe conocer la directiva de contraseñas de vCenter Single Sign-On, de las contraseñas de vCenter Server y el comportamiento de bloqueo.

En esta sección se analizan las contraseñas de vCenter Single Sign-On. Consulte Bloqueo de cuenta y contraseñas ESXi, donde se analizan las contraseñas de los usuarios locales de ESXi.

Requisitos de contraseña de administrador de vCenter Single Sign-On

La contraseña predeterminada del administrador de vCenter Single Sign-On, administrator@vsphere.local, se especifica en la directiva de contraseñas de vCenter Single Sign-On. De manera predeterminada, esta contraseña debe cumplir con los siguientes requisitos:

- Al menos ocho caracteres
- Tener al menos un carácter en minúscula
- Tener al menos un carácter numérico
- Tener al menos un carácter especial

La contraseña de este usuario no puede superar los 20 caracteres. Se permiten caracteres que no sean ASCII. Los administradores pueden cambiar la directiva de contraseñas predeterminada. Consulte la documentación de *vSphere Authentication*.

Requisitos de contraseña de vCenter Server

En vCenter Server, los requisitos de contraseña se determinan mediante vCenter Single Sign-On o por el origen de identidad configurada, que puede ser Active Directory u OpenLDAP.

Comportamiento de bloqueo de vCenter Single Sign-On

Los usuarios quedan bloqueados después de una cantidad preestablecida de intentos consecutivos con errores. De manera predeterminada, los usuarios quedan bloqueados después de cinco intentos consecutivos fallidos en tres minutos, y una cuenta bloqueada se desbloquea automáticamente transcurridos cinco minutos. Se pueden cambiar estos valores predeterminados a través de la directiva de bloqueo de vCenter Single Sign-On. Consulte la documentación de *vSphere Authentication*.

El administrador de dominio de vCenter Single Sign-On, el cual es administrator@vsphere.local de manera predeterminada, no se verá afectado por la directiva de bloqueo. El usuario se ve afectado por la directiva de contraseñas.

Cambios de contraseña de vCenter Server

Si conoce su contraseña, puede cambiarla mediante el comando `dir-cli password change`. Si olvida su contraseña, un administrador de vCenter Single Sign-On puede restablecerla con el comando `dir-cli password reset`.

Busque información acerca de la caducidad de la contraseña y temas relacionados de diversas versiones de vSphere en la base de conocimientos de VMware.

Comprobar huellas digitales para hosts ESXi heredados

En vSphere 6,0 y las versiones posteriores, se asignan certificados de VMCA a los hosts de forma predeterminada. Si cambia el modo de certificación a Huella digital, puede continuar usando este modo para los hosts heredados. Puede comprobar las huellas digitales en vSphere Client.

Nota De manera predeterminada, los certificados se conservan en todas las actualizaciones.

Procedimiento

1 Desplácese hasta vCenter Server en el inventario de vSphere Client.

2 Haga clic en **Configurar**.

3 En **Configuración**, haga clic en **General**.

4 Haga clic en **Editar**.

5 Haga clic en **Configuración de SSL**.

6 Si alguno de los hosts ESXi 5.5 o de versiones anteriores necesita una validación manual, compare las huellas digitales detalladas para los hosts con las huellas digitales de la consola del host.

   Para obtener la huella digital del host, use la interfaz de usuario de la consola directa (DCUI).

   a Inicie sesión en la consola directa y presione F2 para acceder al menú Personalización del sistema.

   b Seleccione **Ver información de soporte**.

      La huella digital del host se muestra en la columna a la derecha.

7 Si la huella digital coincide, active la casilla **Comprobar** ubicada junto al host.

   Los hosts no seleccionados se desconectan después de hacer clic en **Aceptar**.

8 Haga clic en **Guardar**.

Puertos necesarios en vCenter Server

El sistema vCenter Server debe poder enviar datos a cada host administrado y recibir datos de vSphere Client. Para permitir las actividades de migración y aprovisionamiento entre los hosts administrados, los hosts de origen y destino deben poder recibir datos entre sí a través de los puertos TCP y UDP predeterminados.

Se puede acceder a vCenter Server a través de los puertos TCP y UDP predeterminados. Si administra componentes de red desde afuera de un firewall, es posible que se le pida que vuelva a configurar el firewall para permitir el acceso en los puertos necesarios. Para obtener la lista de todos los puertos y protocolos compatibles en vSphere, consulte la herramienta VMware Ports and Protocols™ en https://ports.vmware.com.

Durante la instalación, si un puerto se encuentra en uso o está bloqueado mediante una lista de no permitidos, el instalador de vCenter Server mostrará un mensaje de error. Debe utilizar otro número de puerto para continuar con la instalación. Hay puertos internos que se utilizan solo para la comunicación entre los procesos.

VMware utiliza los puertos designados para la comunicación. Además, los hosts administrados supervisan los puertos designados para los datos desde vCenter Server. Si existe un firewall integrado entre cualquiera de estos elementos, el instalador abre los puertos durante el proceso de instalación o actualización. En el caso de firewalls personalizados, debe abrir manualmente los puertos requeridos. Si posee un firewall entre dos hosts administrados y desea realizar actividades en el origen o destino, como la migración o clonación, debe configurar un medio para que los hosts administrados puedan recibir datos.

Para configurar el sistema vCenter Server a fin de que utilice un puerto diferente donde recibir los datos de vSphere Client, consulte la documentación de *Administrar vCenter Server y hosts*.

Proteger máquinas virtuales

5

El sistema operativo invitado que se ejecuta en la máquina virtual está sujeto a los mismos riesgos de seguridad que un sistema físico. Proteja las máquinas virtuales como se protegen las máquinas físicas. Siga las prácticas recomendadas que se describen en este documento y en la *guía de configuración de seguridad* (anteriormente denominada la *Guía de fortalecimiento*).

La *guía de configuración de seguridad* está disponible en https://core.vmware.com/security.

Lea los siguientes temas a continuación:

- Activar o desactivar el arranque seguro UEFI para una máquina virtual
- Prácticas recomendadas de seguridad para las máquinas virtuales
- Proteger máquinas virtuales con Intel Software Guard Extensions
- Proteger máquinas virtuales con virtualización cifrada segura de AMD: estado cifrado

Activar o desactivar el arranque seguro UEFI para una máquina virtual

El arranque seguro UEFI es un estándar de seguridad que permite garantizar que el equipo arranque usando solamente software de confianza para el fabricante del equipo. Para ciertos sistemas operativos y versiones de hardware de máquinas virtuales, se puede activar el arranque seguro del mismo modo que para una máquina física.

En un sistema operativo que admite el arranque seguro UEFI, cada parte del software de arranque está firmada, incluidos el cargador de arranque, el kernel del sistema operativo y los controladores del sistema operativo. La configuración predeterminada de la máquina virtual incluye varios certificados de firma de código.

- Un certificado de Microsoft que se utiliza solamente para el arranque de Windows.
- Un certificado de Microsoft que se utiliza para código de terceros firmado por Microsoft, como los cargadores de arranque de Linux.
- Un certificado de VMware que solo se utiliza para el arranque de ESXi dentro de una máquina virtual.

La configuración predeterminada de la máquina virtual incluye un certificado para que las solicitudes de autenticación modifiquen la configuración de arranque seguro, incluida la lista de revocación de arranque seguro, desde el interior de la máquina virtual. Se trata de un certificado de clave de intercambio de claves (Key Exchange Key, KEK) de Microsoft.

Se requiere la versión 10.1 o posterior de VMware Tools para las máquinas virtuales que utilizan el arranque seguro UEFI. Puede actualizar esas máquinas virtuales a una versión posterior de VMware Tools cuando esté disponible.

Para las máquinas virtuales Linux, no se admite VMware Host-Guest Filesystem en el modo de arranque seguro. Quite VMware Host-Guest Filesystem de VMware Tools antes de activar el arranque seguro.

Nota Si activa el arranque seguro de una máquina virtual, solo puede cargar controladores firmados en ella.

En esta tarea se describe cómo usar vSphere Client para activar y desactivar el arranque seguro de una máquina virtual. También puede escribir scripts para administrar la configuración de la máquina virtual. Por ejemplo, puede automatizar el cambio del firmware de BIOS a EFI para máquinas virtuales con el siguiente código de PowerCLI:

```
$vm = Get-VM TestVM

$spec = New-Object VMware.Vim.VirtualMachineConfigSpec
$spec.Firmware = [VMware.Vim.GuestOsDescriptorFirmwareType]::efi
$vm.ExtensionData.ReconfigVM($spec)
```

Para obtener más información, consulte la *Guía del usuario de VMware PowerCLI*.

Requisitos previos

Puede activar el arranque seguro solamente si se cumplen los requisitos previos. Si no se cumplen, la casilla no estará visible en vSphere Client.

- Compruebe que el sistema operativo y el firmware de la máquina virtual admitan el arranque UEFI.
  - Firmware EFI.
  - Versión de hardware virtual 13 o posterior.
  - Sistema operativo que admita el arranque seguro UEFI.

  Nota Algunos sistemas operativos invitados no permiten cambiar el arranque del BIOS por el arranque UEFI sin realizar modificaciones al sistema operativo invitado. Consulte la documentación del sistema operativo invitado antes de cambiar al arranque UEFI. Si se actualiza una máquina virtual que ya utiliza el arranque UEFI a un sistema operativo que admite el arranque seguro UEFI, se puede activar el arranque seguro de esa máquina virtual.

- Apague la máquina virtual. Si la máquina virtual está en ejecución, la casilla aparece atenuada.

Procedimiento

1. Desplácese hasta la máquina virtual en el inventario de vSphere Client.
2. Haga clic con el botón derecho en la máquina virtual y seleccione **Editar configuración**.
3. Haga clic en la pestaña **Opciones de máquina virtual** y expanda **Opciones de arranque**.
4. En **Opciones de arranque**, asegúrese de que el firmware esté establecido en **EFI**.
5. Seleccione la tarea en cuestión.
   - Seleccione la casilla **Arranque seguro** para activar el arranque seguro.
   - Anule la selección de la casilla **Arranque seguro** para desactivar el arranque seguro.
6. Haga clic en **Aceptar**.

Resultados

Cuando la máquina virtual arranca, solo se permiten los componentes con firmas válidas. El proceso de arranque se detiene y muestra un error si detecta que existe un componente al que le falta una firma o cuya firma no es válida.

Prácticas recomendadas de seguridad para las máquinas virtuales

Seguir las prácticas recomendadas de seguridad para las máquinas virtuales ayuda a garantizar la integridad de la implementación de vSphere.

- Protección general de la máquina virtual

  La máquina virtual es, en muchos aspectos, el equivalente a un servidor físico. Implemente las mismas medidas de seguridad en las máquinas virtuales que las que implementa en los sistemas físicos.

- Usar plantillas para implementar máquinas virtuales

  Cuando instala manualmente sistemas operativos invitados y aplicaciones en una máquina virtual, se introduce el riesgo de una configuración incorrecta. Mediante el uso de una plantilla que captura la imagen del sistema operativo base, protegido, sin aplicaciones instaladas, es posible garantizar que todas las máquinas virtuales se creen con un nivel de línea base conocido de seguridad.

- Minimizar el uso de la consola de la máquina virtual

  La consola de máquina virtual cumple la misma función en la máquina virtual que el monitor de un servidor físico. Los usuarios que tienen acceso a la consola de la máquina virtual tienen acceso a la administración de energía de la máquina virtual y a los controles de conectividad del dispositivo extraíble. Por lo tanto, el acceso a la consola puede permitir que ocurra un ataque malicioso en una máquina virtual.

- Evitar que las máquinas virtuales asuman el control de los recursos

  Cuando una máquina virtual consume tantos recursos del host que las demás máquinas virtuales presentes en el host no pueden realizar sus respectivas funciones, es posible que se produzca una denegación de servicio (DoS). Para evitar que una máquina virtual provoque una DoS, use las características de administración de recursos del host, como los recursos compartidos de configuración y los grupos de recursos.

- Desactivar funciones innecesarias en máquinas virtuales

  Cualquier servicio que se ejecute en una máquina virtual conlleva un potencial de ataque. Al desactivar los componentes del sistema que no son necesarios para admitir la aplicación o el servicio que está en ejecución en el sistema, se reduce ese potencial.

Protección general de la máquina virtual

La máquina virtual es, en muchos aspectos, el equivalente a un servidor físico. Implemente las mismas medidas de seguridad en las máquinas virtuales que las que implementa en los sistemas físicos.

Siga estas prácticas recomendadas para proteger sus máquinas virtuales. Para obtener más información, consulte la *Guía de configuración de seguridad de vSphere* en https://core.vmware.com/security-configuration-guide.

Revisar máquinas virtuales

Mantenga todas las medidas de seguridad actualizadas, incluidas las revisiones adecuadas. Realice un seguimiento de las actualizaciones para las máquinas virtuales inactivas que están apagadas, ya que podrían pasarse por alto. Por ejemplo, asegúrese de que el software antivirus, el software antispyware, la detección de intrusos y otros tipos de protección estén habilitados para las máquinas virtuales de la infraestructura virtual. También debe asegurarse de tener suficiente espacio para los registros de las máquinas virtuales.

Buscar virus en las máquinas virtuales

Debido a que las máquinas virtuales alojan un sistema operativo estándar, se deben proteger contra virus con un software antivirus. Según cómo utilice la máquina virtual, es posible que también tenga que instalar un firewall de software.

Escalone la programación de análisis de virus, particularmente en las implementaciones que tengan gran cantidad de máquinas virtuales. El rendimiento de los sistemas en el entorno disminuye notablemente si examina todas las máquinas virtuales a la vez. Como los firewalls de software y los software antivirus pueden tener un gran consumo de la capacidad de virtualización, equilibre el uso de estas dos medidas de seguridad según el rendimiento de las máquinas virtuales, en especial si sabe que las máquinas virtuales están en un entorno de plena confianza.

Desactivar puertos serie en máquinas virtuales

Los puertos serie son interfaces para conectar periféricos con la máquina virtual. Los administradores suelen utilizar puertos serie para proporcionar una conexión directa de bajo nivel a la consola de un servidor. Un puerto serie virtual permite el mismo acceso a una máquina virtual. Dado que los puertos serie permiten el acceso de bajo nivel y no tienen controles sólidos, como registros o privilegios, mantenga los puertos desactivados en las máquinas virtuales.

Usar plantillas para implementar máquinas virtuales

Cuando instala manualmente sistemas operativos invitados y aplicaciones en una máquina virtual, se introduce el riesgo de una configuración incorrecta. Mediante el uso de una plantilla que captura la imagen del sistema operativo base, protegido, sin aplicaciones instaladas, es posible garantizar que todas las máquinas virtuales se creen con un nivel de línea base conocido de seguridad.

Puede utilizar plantillas que contengan un sistema operativo protegido, revisado y adecuadamente configurado para crear otras plantillas específicas de la aplicación, o bien puede utilizar la plantilla de la aplicación para implementar máquinas virtuales.

Procedimiento

- Proporcione plantillas para la creación de máquinas virtuales que contengan implementaciones de sistemas operativos protegidos, revisados y adecuadamente configurados.

  De ser posible, también implemente aplicaciones en las plantillas. Asegúrese de que las aplicaciones no dependan de la información específica de la máquina virtual para poder implementarlas.

Pasos siguientes

Para obtener más información sobre las plantillas, consulte la documentación de *Administrar máquinas virtuales de vSphere*.

Minimizar el uso de la consola de la máquina virtual

La consola de máquina virtual cumple la misma función en la máquina virtual que el monitor de un servidor físico. Los usuarios que tienen acceso a la consola de la máquina virtual tienen acceso a la administración de energía de la máquina virtual y a los controles de conectividad del dispositivo extraíble. Por lo tanto, el acceso a la consola puede permitir que ocurra un ataque malicioso en una máquina virtual.

Procedimiento

1 Utilice servicios nativos de administración remota, como servicios de terminal y SSH, para interactuar con las máquinas virtuales.

  Otorgue acceso a la consola de máquina virtual solo cuando sea necesario.

2 Limite las conexiones a la consola de máquina virtual.

   Por ejemplo, en un entorno muy seguro, limítela a una conexión. En algunos entornos, se puede incrementar el límite si se necesitan varias conexiones simultáneas para realizar las tareas normales.

   a En vSphere Client, apague la máquina virtual.

   b Haga clic con el botón derecho en la máquina virtual y seleccione **Editar configuración**.

   c Haga clic en la pestaña **Opciones de máquina virtual** y amplíe **Opciones de VMware Remote Console**.

   d Introduzca la cantidad máxima de sesiones (por ejemplo, **2**).

   e Haga clic en **Aceptar**.

Evitar que las máquinas virtuales asuman el control de los recursos

Cuando una máquina virtual consume tantos recursos del host que las demás máquinas virtuales presentes en el host no pueden realizar sus respectivas funciones, es posible que se produzca una denegación de servicio (DoS). Para evitar que una máquina virtual provoque una DoS, use las características de administración de recursos del host, como los recursos compartidos de configuración y los grupos de recursos.

De forma predeterminada, todas las máquinas virtuales de un host ESXi comparten los recursos de forma equitativa. Puede utilizar los recursos compartidos y los grupos de recursos para evitar un ataque por denegación de servicio que haga que una máquina virtual consuma tantos recursos del host que las demás máquinas virtuales del mismo host no puedan realizar sus respectivas funciones.

No establezca límites ni utilice grupos de recursos hasta que comprenda completamente el impacto.

Procedimiento

1 Aprovisione cada máquina virtual solo con los recursos (CPU y memoria) suficientes para que funcione de forma adecuada.

2 Utilice los recursos compartidos para garantizar que las máquinas virtuales fundamentales tengan los recursos necesarios.

3 Agrupe las máquinas virtuales con requisitos similares en grupos de recursos.

4 En cada grupo de recursos, deje la opción de recursos compartidos con los valores predeterminados para que cada máquina virtual del grupo tenga aproximadamente la misma prioridad de recursos.

   Con esta configuración, una máquina virtual individual no puede usar más recursos que las demás máquinas virtuales del grupo de recursos.

Pasos siguientes

Consulte la documentación de *Administrar recursos de vSphere* para obtener información sobre recursos compartidos y límites.

Desactivar funciones innecesarias en máquinas virtuales

Cualquier servicio que se ejecute en una máquina virtual conlleva un potencial de ataque. Al desactivar los componentes del sistema que no son necesarios para admitir la aplicación o el servicio que está en ejecución en el sistema, se reduce ese potencial.

Las máquinas virtuales no suelen precisar tantos servicios o tantas funciones como los servidores físicos. A la hora de virtualizar un sistema, evalúe si es necesario ese servicio o esa función en particular.

Nota Cuando sea posible, instale sistemas operativos invitados mediante los modos de instalación "mínimo" o "básico" para reducir el tamaño, la complejidad y la superficie de ataque del sistema operativo invitado.

Procedimiento

- Desactive los servicios que no se utilizan en el sistema operativo.

  Por ejemplo, si el sistema ejecuta un servidor de archivos, desconecte los servicios web.
- Desconecte los dispositivos físicos que no se utilizan, como unidades de CD/DVD, unidades de disquete y adaptadores USB.
- Desactive las funcionalidades que no se utilicen, como las funciones de visualización que no se utilizan (o Carpetas compartidas de VMware), las cuales permiten compartir archivos de host con la máquina virtual (sistema de archivos invitado del host).
- Apague los protectores de pantalla.
- No ejecute el sistema X Window en los sistemas operativos invitados Linux, BSD o Solaris a menos que sea necesario.

Eliminar dispositivos de hardware innecesarios de máquinas virtuales

Cualquier dispositivo activado o conectado en una máquina virtual representa un canal de ataque potencial. Los usuarios y los procesos con privilegios sobre una máquina virtual pueden conectar o desconectar dispositivos de hardware, como adaptadores de red o unidades de CD-ROM. Los atacantes pueden usar esta funcionalidad para infringir la seguridad de la máquina virtual. La eliminación de los dispositivos de hardware innecesarios permite evitar ataques.

Un atacante con acceso a una máquina virtual puede conectar o desconectar un dispositivo de hardware y acceder a información confidencial en un soporte físico que quede en un dispositivo de hardware. El atacante puede llegar a desconectar un adaptador de red para aislar la máquina virtual de su red, mediante lo cual se puede producir una denegación de servicio.

- No conecte dispositivos no autorizados a la máquina virtual.

- Elimine los dispositivos de hardware que no necesite o que no esté usando.
- Desactivar dispositivos virtuales innecesarios desde una máquina virtual.
- Asegúrese de que solo los dispositivos necesarios estén conectados a una máquina virtual. Rara vez las máquinas virtuales utilizan puertos serie o paralelos. Como regla general, las unidades de CD/DVD solo se conectan temporalmente durante la instalación del software.

Procedimiento

1 Desplácese hasta la máquina virtual en el inventario de vSphere Client.

2 Haga clic con el botón derecho en la máquina virtual y, a continuación, haga clic en **Editar configuración**.

3 En la pestaña **Hardware virtual**, haga clic en el icono de puntos suspensivos y seleccione **Quitar dispositivo** para desactivar los dispositivos de hardware que no sean necesarios.

   Compruebe también los siguientes dispositivos:

   - Puertos serie
   - Puertos paralelos
   - controladoras USB
   - unidades de CD-ROM

   Nota Para administrar dispositivos de unidad de disquete en vSphere 7.0 y versiones posteriores tiene que utilizar comandos PowerCLI.

Desactivar funciones de visualización no utilizadas en máquinas virtuales

Los atacantes pueden aprovechar una característica de visualización que no se utiliza para introducir un código malicioso en el entorno. Desactive las funciones que no estén en uso en su entorno.

Requisitos previos

Apague la máquina virtual.

Procedimiento

1 Desplácese hasta la máquina virtual en el inventario de vSphere Client.

2 Haga clic con el botón derecho en la máquina virtual y, a continuación, haga clic en **Editar configuración**.

3 Seleccione **Parámetros avanzados**.

4 Si corresponde, agregue o edite los siguientes parámetros.

Nombre	Descripción
svga.vgaonly	Si establece este parámetro en el valor TRUE, las funciones avanzadas de gráficos dejarán de funcionar. No establezca este parámetro como TRUE con sistemas operativos invitados actuales, ya que no funcionan correctamente. Cuando `svga.vgaonly` se establece como TRUE, solo está disponible el modo de consola de celdas de caracteres. Si utiliza esta configuración, `mks.enable3d` no tendrá efecto. **Nota** Aplique esta configuración únicamente a las máquinas virtuales que no necesitan una tarjeta de video virtualizada.
mks.enable3d	Establezca este parámetro en el valor FALSE en las máquinas virtuales que no necesitan la funcionalidad 3D.

5 Haga clic en **Aceptar**.

Desactivar las operaciones para copiar y pegar entre el sistema operativo invitado y la consola remota

Las operaciones para copiar y pegar entre el sistema operativo invitado y la consola remota están desactivadas de forma predeterminada. Para lograr un entorno seguro, conserve la configuración predeterminada. Si necesita utilizar las operaciones para copiar y pegar, debe activarlas por medio de vSphere Client.

Los valores predeterminados de estas opciones se establecen para garantizar un entorno seguro. Sin embargo, debe establecerlas en True de forma explícita para que las herramientas de auditoría puedan comprobar que la configuración sea correcta.

Requisitos previos

Apague la máquina virtual.

Procedimiento

1 Desplácese hasta la máquina virtual en el inventario de vSphere Client.

2 Haga clic con el botón derecho en la máquina virtual y, a continuación, haga clic en **Editar configuración**.

3 Seleccione **Parámetros avanzados**.

4 Agregue o edite los siguientes parámetros.

Nombre	Valor
`isolation.tools.copy.disable`	`true`
`isolation.tools.paste.disable`	`true`
`isolation.tools.setGUIOptions.enable`	`false`

Estas opciones anulan la configuración realizada en el panel de control de VMware Tools del sistema operativo invitado.

5 Haga clic en **Aceptar**.

6 (opcional) Si realizó cambios en los parámetros de configuración, reinicie la máquina virtual.

Limitar la exposición de los datos confidenciales copiados al portapapeles de la consola de máquina virtual

De forma predeterminada, las operaciones para copiar y pegar están desactivadas para los hosts a fin de evitar la exposición de los datos confidenciales que se copiaron al portapapeles.

Cuando la función de copiar y pegar está activada en una máquina virtual que ejecuta VMware Tools, se pueden copiar y pegar elementos entre el sistema operativo invitado y la consola remota. Cuando se centra la atención sobre la ventana de la consola, los procesos que se ejecutan en la máquina virtual y los usuarios sin privilegios pueden acceder al portapapeles de la consola de la máquina virtual. Si un usuario copia información confidencial en el portapapeles antes de utilizar la consola, el usuario podrá exponer datos confidenciales a la máquina virtual. Para evitar este problema, las operaciones para copiar y pegar del sistema operativo invitado están desactivadas de forma predeterminada.

De ser necesario, es posible activarlas para las máquinas virtuales.

Restringir la ejecución de comandos dentro de una máquina virtual a los usuarios

De forma predeterminada, un usuario con la función Administrador de vCenter Server puede interactuar con archivos y aplicaciones dentro del sistema operativo invitado de una máquina virtual. Para reducir el riesgo de infracciones de confidencialidad, disponibilidad o integridad del invitado, cree una función de acceso que no sea de invitado en la que no esté el privilegio **Máquina virtual.Operaciones de invitado**. Asigne esa función a los administradores que no necesiten acceso a archivos de máquinas virtuales.

Por motivos de seguridad, aplique las mismas restricciones en los permisos de acceso al centro de datos virtual que en el centro de datos físico. Aplique una función personalizada que no incluya el privilegio **Máquina virtual.Operaciones de invitado** a los usuarios que necesiten privilegios de administrador, pero que no estén autorizados a interactuar con archivos y aplicaciones del sistema operativo invitado.

Por ejemplo, la configuración puede incluir una máquina virtual en la infraestructura que tenga información confidencial.

Si tareas como la migración de vMotion necesitan que los administradores de centros de datos puedan acceder a la máquina virtual, desactive algunas operaciones remotas del sistema operativo invitado para garantizar que esos administradores no puedan acceder a información confidencial.

Requisitos previos

Compruebe que tenga privilegios de **Administrador** en el sistema vCenter Server en el que crea el rol.

Procedimiento

1 Inicie sesión en vSphere Client como un usuario con privilegios de **Administrador** en el sistema vCenter Server donde desea crear la función.

2 Seleccione **Administración** y haga clic en **Funciones**.

3 Haga clic en la función Administrador y en **Clonar**.

4 Introduzca un nombre de función y una descripción, y haga clic en **Aceptar**.

   Por ejemplo, escriba **`Acceso de administrador no invitado`**.

5 Seleccione la función clonada y haga clic en **Editar**.

6 En el privilegio **Máquina virtual**, anule la selección de Operaciones de invitado.

7 Haga clic en **Guardar**.

Pasos siguientes

Seleccione el sistema vCenter Server o el host, y asigne un permiso que se asocie con el usuario o el grupo que debe tener los nuevos privilegios con la función recién creado. Quite esos usuarios de la función Administrador.

Evitar que un usuario o proceso de máquina virtual desconecten dispositivos

Los usuarios y los procesos sin privilegios de raíz o administrador en máquinas virtuales pueden conectar o desconectar dispositivos, como adaptadores de red y unidades de CD-ROM, y pueden modificar la configuración de los dispositivos. Para mejorar la seguridad de la máquina virtual, quite estos dispositivos.

Puede evitar que los usuarios de la máquina virtual en el sistema operativo invitado y los procesos que se ejecutan en el sistema operativo invitado modifiquen los dispositivos mediante cambios en la configuración avanzada de la máquina virtual.

Requisitos previos

Apague la máquina virtual.

Procedimiento

1 Desplácese hasta la máquina virtual en el inventario de vSphere Client.

2 Haga clic con el botón derecho en la máquina virtual y, a continuación, haga clic en **Editar configuración**.

3 Haga clic en la pestaña **Parámetros avanzados**.

4 Compruebe el siguiente parámetro o agréguelo.

Nombre	Valor
isolation.device.connectable.disable	true

Esta opción no afecta a la capacidad del administrador de vSphere para conectar o desconectar los dispositivos conectados a la máquina virtual.

5 Haga clic en **Aceptar**.

Evitar que los procesos del sistema operativo invitado envíen mensajes de configuración al host

Para asegurarse de que el sistema operativo invitado no modifique los parámetros de configuración, se puede evitar que estos procesos escriban cualquier par nombre-valor en el archivo de configuración.

Requisitos previos

Apague la máquina virtual.

Procedimiento

1 Desplácese hasta la máquina virtual en el inventario de vSphere Client.

2 Haga clic con el botón derecho en la máquina virtual y, a continuación, haga clic en **Editar configuración**.

3 Seleccione **Parámetros avanzados**.

4 Compruebe el siguiente parámetro o agréguelo.

Nombre	Valor
isolation.tools.setinfo.disable	true

5 Haga clic en **Aceptar**.

Evitar el uso de discos independientes no persistentes con máquinas virtuales

Al utilizar discos independientes no persistentes con máquinas virtuales, los atacantes exitosos pueden apagar o reiniciar el sistema y así eliminar cualquier evidencia de que la máquina fue vulnerada. Sin un registro persistente de la actividad de la máquina virtual, los administradores podrían desconocer el ataque. Por lo tanto, evite utilizar discos independientes no persistentes .

Procedimiento

1 Asegúrese de que la actividad de la máquina virtual se registre de forma remota en un servidor separado, como un servidor syslog o un recopilador de eventos basado en Windows.

2 Si el registro remoto de eventos y de actividad no está configurado para el invitado, asegúrese de que scsiX:Y.mode está configurado de una de las siguientes formas:

- No presente
- No establecido en independiente no persistente

Resultados

Cuando el modo no persistente no está habilitado, no se puede revertir la máquina virtual a un estado conocido al reiniciar el sistema.

Proteger máquinas virtuales con Intel Software Guard Extensions

vSphere permite configurar varias instancias de Virtual Intel® Software Guard Extension (vSGX) para máquinas virtuales. Con vSGX, puede proporcionar seguridad adicional a las cargas de trabajo.

Algunas CPU modernas de Intel implementan una extensión de seguridad llamada Intel® Software Guard Extensions (Intel® SGX). Intel SGX es una tecnología específica del procesador para desarrolladores de aplicaciones que buscan proteger determinados códigos y datos evitar para evitar su divulgación o modificación. Intel SGX permite código a nivel de usuario para definir regiones privadas de memoria, denominadas enclaves. El contenido de los enclaves está protegido de manera tal que el código que se ejecuta fuera de enclave no puede acceder al contenido del enclave.

vSGX permite que las máquinas virtuales utilicen la tecnología Intel SGX si está disponibles en el hardware. Para usar vSGX, el host ESXi debe estar instalado en una CPU compatible con SGX, y SGX debe estar habilitado en el BIOS del host ESXi. Puede utilizar vSphere Client para habilitar SGX para una máquina virtual.

En vSphere 8.0 y versiones posteriores, puede utilizar la atestación remota para una máquina virtual habilitada para vSGX. La atestación remota Intel SGX es un mecanismo de seguridad que permite establecer un canal de comunicación autenticado y seguro con una entidad remota de confianza. Para utilizar la atestación remota para máquinas virtuales que usan enclaves de SGX, los hosts con un solo socket de CPU no requieren registro en Intel. Para habilitar la atestación remota en una máquina virtual que se ejecuta en un host con varios sockets de CPU, primero debe registrar el host con el servidor de registro de Intel. Si un host compatible con SGX con varios sockets de CPU no está registrado en el servidor de registro de Intel, solo podrá encender máquinas virtuales habilitadas para vSGX que no requieran atestación remota.

Consulte la documentación de *Administrar vCenter Server y hosts* para obtener más información sobre el registro de un host ESXi de varios sockets en el servidor de registro de Intel.

Introducción a vSGX

Las máquinas virtuales pueden usar la tecnología Intel SGX, si está disponible en el hardware.

Requisitos de vSphere para vSGX

Para utilizar vSGX, el entorno de vSphere debe cumplir con estos requisitos:

- Requisitos de la máquina virtual:
  - Firmware EFI.
  - Versión de hardware 17 o posterior
  - Para habilitar la atestación remota, la versión 20 o posterior de hardware
- Requisitos de los componentes:
  - vCenter Server 7.0 y versiones posteriores
  - ESXi 7.0 y versiones posteriores
  - El host ESXi debe estar instalado en una CPU compatible con SGX y SGX debe estar habilitado en el BIOS del host ESXi.
  - Para habilitar la atestación remota para el host, registre el host con el servidor de registro de Intel. De esta manera, la máquina virtual que se ejecuta en el host puede utilizar la atestación remota. Para obtener más información sobre cómo registrar un ESXi de varios sockets, consulte la documentación de *Administrar vCenter Server y hosts*.
- Compatibilidad con el sistema operativo invitado:
  - Linux
  - Windows Server 2016 (64 bits) y versiones posteriores
  - Windows 10 (64 bits) y versiones posteriores

Hardware Intel compatible con vSGX

Para obtener información sobre el hardware Intel compatible con vSGX, consulte la Guía de compatibilidad de vSphere en https://www.vmware.com/resources/compatibility/search.php.

Es posible que deba desactivar el hiperproceso en ciertas CPU para habilitar SGX en el host ESXi. Para obtener más información, consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/71367.

Funciones de VMware no admitidas en vSGX

Las siguientes funciones no se admiten en una máquina virtual cuando se habilita vSGX:

- Migración de vMotion/DRS
- Suspensión y reanudación de la máquina virtual
- Instantáneas de máquina virtual (estas instantáneas son compatibles si no se realiza una instantánea de la memoria de la máquina virtual).
- Tolerancia a errores

- Integridad del invitado (GI, base de la plataforma para VMware AppDefense™ 1.0)

Nota Estas funciones de VMware no se admiten debido al modo en que funciona la arquitectura de Intel SGX. No son resultado de un defecto de VMware.

Habilitar vSGX en una máquina virtual

Puede habilitar vSGX en una máquina virtual al mismo tiempo que crea una máquina virtual.

Requisitos previos

Consulte Requisitos de vSphere para vSGX.

Procedimiento

1 Conéctese a vCenter Server mediante vSphere Client.

2 Seleccione un objeto del inventario que sea un objeto primario válido de una máquina virtual, por ejemplo, un host o clúster ESXi.

3 Haga clic con el botón derecho en el objeto, seleccione **Nueva máquina virtual** y siga las indicaciones para crear una máquina virtual.

4 En la página **Personalizar hardware**, haga clic en la pestaña **Hardware virtual** y expanda **Dispositivos de seguridad**.

5 Para habilitar SGX, active la casilla **Habilitar**.

6 En el cuadro de texto **Tamaño de memoria caché de página de enclave (MB)**, introduzca el tamaño de la caché en MB.

   Nota El tamaño de la memoria caché de la página enclave debe ser un múltiplo de 2 MB.

7 Para evitar que la máquina virtual encienda hosts que no admiten la atestación remota de SGX, como hosts SGX de varios sockets no registrados, active la casilla de verificación **Atestación remota**.

8 En el menú desplegable **Configuración de control de inicio**, seleccione el modo adecuado.

Opción	Acción
Desbloqueado	Esta opción habilita la configuración de enclave de inicio del sistema operativo invitado.
Bloqueado	Esta opción permite configurar el enclave de inicio. a Seleccione la opción **Hash de clave pública de enclave de inicio**. b Para utilizar una de las claves públicas configuradas en el host, seleccione **Utilizar a partir del host** y, en el menú desplegable, seleccione un hash de clave pública. c Para introducir la clave pública manualmente, seleccione **Introducir manualmente** y escriba una clave de caracteres hash SHA256 (64) válida.

9 Haga clic en **Aceptar**.

Habilitar vSGX en una máquina virtual existente

Puede habilitar vSGX en una máquina virtual existente.

Requisitos previos

Consulte Requisitos de vSphere para vSGX.

Procedimiento

1 Conéctese a vCenter Server mediante vSphere Client.

2 Haga clic con el botón derecho en la máquina virtual en el inventario que desee modificar y seleccione **Editar configuración**.

3 En la pestaña **Hardware virtual**, expanda **Dispositivos de seguridad**.

4 Para habilitar SGX, active la casilla **Habilitar**.

5 En el cuadro de texto **Tamaño de memoria caché de página de enclave (MB)**, introduzca el tamaño de la caché en MB.

Nota El tamaño de la memoria caché de la página enclave debe ser un múltiplo de 2 MB.

6 Para evitar que la máquina virtual encienda hosts que no admiten la atestación remota de SGX, como hosts SGX de varios sockets no registrados, active la casilla de verificación **Atestación remota**.

7 En el menú desplegable **Configuración de control de inicio**, seleccione el modo adecuado.

Opción	Acción
Desbloqueado	Esta opción habilita la configuración de enclave de inicio del sistema operativo invitado.
Bloqueado	Esta opción permite configurar el enclave de inicio. a Seleccione la opción **Hash de clave pública de enclave de inicio**. b Para utilizar una de las claves públicas configuradas en el host, seleccione **Utilizar a partir del host** y, en el menú desplegable, seleccione un hash de clave pública. c Para introducir la clave pública manualmente, seleccione **Introducir manualmente** y escriba una clave de caracteres hash SHA256 (64) válida.

8 Haga clic en **Aceptar**.

Eliminar vSGX de una máquina virtual

Puede eliminar vSGX de una máquina virtual.

Procedimiento

1 Conéctese a vCenter Server mediante vSphere Client.

2 Haga clic con el botón derecho en la máquina virtual en el inventario que desee modificar y seleccione **Editar configuración**.

3 En el cuadro de diálogo **Editar configuración**, en **Dispositivos de seguridad**, anule la selección de la casilla **Habilitar** para SGX.

4 Haga clic en **Aceptar**.

   Compruebe que la entrada de vSGX ya no aparezca en la pestaña **Resumen** de la máquina virtual en el panel **Hardware de máquina virtual**.

Proteger máquinas virtuales con virtualización cifrada segura de AMD: estado cifrado

Virtualización cifrada segura de AMD - Estado cifrad (SEV-ES) es una función de hardware habilitada en las CPU de AMD recientes que mantiene la memoria del sistema operativo invitado y el estado de registro cifrado, lo que protege el acceso del hipervisor.

Puede agregar SEV-ES a las máquinas virtuales como una mejora de seguridad adicional. SEV-ES impide que los registros de la CPU filtren información en los registros de los componentes como el hipervisor. SEV-ES también puede detectar modificaciones malintencionadas en un estado de registro de la CPU.

vSphere y estado cifrado de Secure Encrypted Virtualization-Encrypted State (SEV-ES) de AMD

En vSphere 7.0 Update 1 y versiones posteriores, se puede activar el estado cifrado de SEV (Secure Encrypted Virtualization-Encrypted State, SEV-ES) en los sistemas operativos invitados y las CPU de AMD compatibles.

En este momento, SEV-ES solo es compatible con las CPU de AMD EPYC 7xx2 (código denominado "Roma") y las CPU posteriores, y solo con las versiones de kernels de Linux que incluyen soporte específico para SEV-ES.

Arquitectura y componentes de SEV-ES

La arquitectura del estado cifrado de SEV (Secure Encrypted Virtualization-Encrypted State, SEV-ES) consta de los siguientes componentes.

- La CPU de AMD, específicamente, el procesador de seguridad de plataforma (Platform Security Processor, PSP) que administra las claves de cifrado y controla el cifrado.
- El sistema operativo habilitado; es decir, un sistema operativo que utiliza llamadas iniciadas por el invitado al hipervisor.
- El monitor de máquina virtual (Virtual Machine Monitor, VMM) y el ejecutable de máquina virtual (Virtual Machine Executable, VMX) para inicializar un estado de una máquina virtual cifrada durante el encendido de la máquina virtual y, asimismo, controlar las llamadas desde el sistema operativo invitado.

- Controlador de VMkernel para comunicar datos no cifrados entre el hipervisor y el sistema operativo invitado.

Implementar y administrar SEV-ES en ESXi

Primero debe activar SEV-ES (el estado cifrado de Secure Encrypted Virtualization) en la configuración BIOS del sistema. Consulte la documentación del sistema para obtener más información sobre cómo acceder a la configuración del BIOS. Después de activar SEV-ES en la BIOS del sistema, podrá agregar SEV-ES a una máquina virtual.

Podrá utilizar vSphere Client (en vSphere 7.0 Update 2 y versiones posteriores) o los comandos de PowerCLI para activar y desactivar SEV-ES en máquinas virtuales. Se pueden crear máquinas virtuales nuevas con SEV-ES o bien se puede activar SEV-ES en las máquinas virtuales existentes. Los privilegios para administrar máquinas virtuales activadas con SEV-ES son los mismos que para administrar máquinas virtuales normales.

Funciones de VMware no admitidas en SEV-ES

Las siguientes funciones no se admiten cuando SEV-ES está activado.

- Modo de administración del sistema
- vMotion
- Instantáneas encendidas (sin embargo, sí se admiten las instantáneas sin memoria)
- La adición o eliminación en caliente de CPU o memoria
- Suspensión o reanudación
- VMware Fault Tolerance
- Clones y clones instantáneos
- Integridad de invitado
- arranque seguro UEFI

Agregar el estado cifrado de SEV (Secure Encrypted Virtualization) de AMD a una máquina virtual mediante vSphere Client

En vSphere 7.0 Update 2 y versiones posteriores, puede utilizar vSphere Client para agregar SEV-ES a una máquina virtual con el fin de proporcionar una mayor seguridad al sistema operativo invitado.

Puede agregar el estado cifrado de SEV (Secure Encrypted Virtualization-Encrypted State, SEV-ES) a las máquinas virtuales que se ejecutan en ESXi 7.0 Update 1 o posterior.

Requisitos previos

- El sistema se debe instalar con una CPU AMD EPYC 7xx2 (código denominado "Roma") o una versión posterior y una BIOS compatible.

- El estado cifrado de SEV (Secure Encrypted Virtualization-Encrypted State, SEV-ES) debe estar habilitado en la BIOS.
- La BIOS controla el número de máquinas virtuales de SEV-ES por host ESXi. Al hacerlo, introduzca un valor para la opción de **ASID mínimo de estado no cifrado de SEV** que sea igual a la cantidad de máquinas virtuales con SEV-ES más una. Por ejemplo, si tiene 12 máquinas virtuales que desee ejecutar de forma simultánea, introduzca **13**.

  Nota vSphere 7.0 Update 1 y versiones posteriores admiten 16 máquinas virtuales habilitadas para SEV-ES por host ESXi. Si se utiliza una configuración más alta en la BIOS, SEV-ES seguirá funcionando, pero se aplica el límite de 16. vSphere 7.0 Update 2 y posteriores admiten 480 máquinas virtuales habilitadas para SEV-ES por host ESXi.

- El host ESXi que se ejecute en el entorno debe ser ESXi 7.0 Update 1 o una versión posterior.
- vCenter Server debe ser vSphere 7.0 Update 2 o una versión posterior.
- El sistema operativo invitado debe ser compatible con el estado cifrado de SEV (Secure Encrypted Virtualization-Encrypted State, SEV-ES).

  Actualmente, solo se admiten kernels de Linux con soporte específico para el estado cifrado de SEV (Secure Encrypted Virtualization-Encrypted State, SEV-ES).
- La máquina virtual debe tener la versión de hardware 18 o una posterior.
- La máquina virtual debe tener habilitada la opción **Reservar toda la memoria de invitado**; de lo contrario, se producirá un error de encendido.

Procedimiento

1 Conéctese a vCenter Server mediante vSphere Client.

2 Seleccione un objeto del inventario que sea un objeto primario válido de una máquina virtual, por ejemplo, un host o clúster ESXi.

3 Haga clic con el botón derecho en el objeto, seleccione **Nueva máquina virtual** y siga las indicaciones para crear una máquina virtual.

Opción	Acción
Seleccionar un tipo de creación	Cree una máquina virtual.
Seleccionar un nombre y una carpeta	Especifique un nombre y una ubicación de destino.
Seleccionar un recurso informático	Especifique el objeto sobre el que tiene privilegios para crear máquinas virtuales.
Seleccionar almacenamiento	En la directiva de almacenamiento de máquina virtual, seleccione la directiva de almacenamiento. Seleccione un almacén de datos compatible.
Seleccionar compatibilidad	Asegúrese de seleccionar **ESXi 7.0 y versiones posteriores**.
Seleccionar un sistema operativo invitado	Seleccione Linux y una versión de Linux con compatibilidad específica para SEV-ES.

Opción	Acción
Personalizar hardware	En **Opciones de máquina virtual > Opciones de arranque > Firmware**, asegúrese de que EFI está seleccionado. En **Opciones de máquina virtual > Cifrado**, seleccione la casilla de verificación **Habilitar** para SEV-ES de AMD.
Listo para finalizar	Revise la información y haga clic en **Finalizar**.

Resultados

La máquina virtual se crea con estado cifrado de SEV (Secure Encrypted Virtualization-Encrypted State, SEV-ES).

Agregar el estado cifrado de SEV (Secure Encrypted Virtualization) de AMD a una máquina virtual mediante la línea de comandos

Puede usar la línea de comandos para agregar el estado cifrado de SEV (Secure Encrypted Virtualization-Encrypted State, SEV-ES) a una máquina virtual para proporcionar mayor seguridad al sistema operativo invitado.

Puede agregar el estado cifrado de SEV (Secure Encrypted Virtualization-Encrypted State, SEV-ES) a las máquinas virtuales que se ejecutan en ESXi 7.0 Update 1 o posterior.

Requisitos previos

- El sistema se debe instalar con una CPU AMD EPYC 7xx2 (código denominado "Roma") o una versión posterior y una BIOS compatible.
- El estado cifrado de SEV (Secure Encrypted Virtualization-Encrypted State, SEV-ES) debe estar habilitado en la BIOS.
- La BIOS controla el número de máquinas virtuales de SEV-ES por host ESXi. Al hacerlo, introduzca un valor para la opción de **ASID mínimo de estado no cifrado de SEV** que sea igual a la cantidad de máquinas virtuales con SEV-ES más una. Por ejemplo, si tiene 12 máquinas virtuales que desee ejecutar de forma simultánea, introduzca **13**.

  Nota vSphere 7.0 Update 1 y versiones posteriores admiten 16 máquinas virtuales habilitadas para SEV-ES por host ESXi. Si se utiliza una configuración más alta en la BIOS, SEV-ES seguirá funcionando, pero se aplica el límite de 16. vSphere 7.0 Update 2 y posteriores admiten 480 máquinas virtuales habilitadas para SEV-ES por host ESXi.

- El host ESXi que se ejecute en el entorno debe ser ESXi 7.0 Update 1 o una versión posterior.
- El sistema operativo invitado debe ser compatible con el estado cifrado de SEV (Secure Encrypted Virtualization-Encrypted State, SEV-ES).

  Actualmente, solo se admiten kernels de Linux con soporte específico para el estado cifrado de SEV (Secure Encrypted Virtualization-Encrypted State, SEV-ES).
- La máquina virtual debe tener la versión de hardware 18 o una posterior.

- La máquina virtual debe tener habilitada la opción **Reservar toda la memoria de invitado**; de lo contrario, se producirá un error de encendido.
- PowerCLI 12.1.0 o una versión posterior debe estar instalada en un sistema con acceso a su entorno.

Procedimiento

1. En una sesión de PowerCLI, ejecute el cmdlet `Connect-VIServer` para conectarse como administrador a la instancia de vCenter Server que administra el host ESXi en el que desea agregar una máquina virtual con SEV-ES.

   ```
   Connect-VIServer -server vCenter_Server_ip_address -User admin_user -Password 'password'
   ```

2. Cree la máquina virtual con el cmdlet `New-VM` y especifique `-SEVEnabled $true`.

   Por ejemplo, asigne primero la información del host a una variable y, a continuación, cree la máquina virtual.

   ```
   $vmhost = Get-VMHost -Name 10.193.25.83
   New-VM -Name MyVM1 $vmhost -NumCPU 2 -MemoryMB 4 -DiskMB 4 -SEVEnabled $true
   ```

   Si debe especificar la versión del hardware virtual, ejecute el cmdlet `New-VM` con el parámetro `-HardwareVersion vmx-18`. Por ejemplo:

   ```
   New-VM -Name MyVM1 $vmhost -NumCPU 2 -MemoryMB 4 -DiskMB 4 -SEVEnabled $true
   -HardwareVersion vmx-18
   ```

Resultados

La máquina virtual se crea con estado cifrado de SEV (Secure Encrypted Virtualization-Encrypted State, SEV-ES).

Activar el estado cifrado de SEV (Secure Encrypted Virtualization) de AMD en una máquina virtual existente mediante vSphere Client

En vSphere 7.0 Update 2 y versiones posteriores, puede utilizar vSphere Client para agregar SEV-ES a una máquina virtual existente con el fin de proporcionar una mayor seguridad al sistema operativo invitado.

Puede agregar el estado cifrado de SEV (Secure Encrypted Virtualization-Encrypted State, SEV-ES) a las máquinas virtuales que se ejecutan en ESXi 7.0 Update 1 o posterior.

Requisitos previos

- El sistema se debe instalar con una CPU AMD EPYC 7xx2 (código denominado "Roma") o una versión posterior y una BIOS compatible.
- El estado cifrado de SEV (Secure Encrypted Virtualization-Encrypted State, SEV-ES) debe estar activado en la BIOS.

- La BIOS controla el número de máquinas virtuales de SEV-ES por host ESXi. Al hacerlo, introduzca un valor para la opción de **ASID mínimo de estado no cifrado de SEV** que sea igual a la cantidad de máquinas virtuales con SEV-ES más una. Por ejemplo, si tiene 12 máquinas virtuales que desee ejecutar de forma simultánea, introduzca **13**.

  Nota vSphere 7.0 Update 1 y versiones posteriores admiten 16 máquinas virtuales activadas para SEV-ES por host ESXi. Si se utiliza una configuración más alta en la BIOS, SEV-ES seguirá funcionando, pero se aplica el límite de 16. vSphere 7.0 Update 2 y posteriores admiten 480 máquinas virtuales activadas para SEV-ES por host ESXi.

- El host ESXi que se ejecute en el entorno debe ser ESXi 7.0 Update 1 o una versión posterior.
- vCenter Server debe ser vSphere 7.0 Update 2 o una versión posterior.
- El sistema operativo invitado debe ser compatible con el estado cifrado de SEV (Secure Encrypted Virtualization-Encrypted State, SEV-ES).

  Actualmente, solo se admiten kernels de Linux con soporte específico para el estado cifrado de SEV (Secure Encrypted Virtualization-Encrypted State, SEV-ES).
- La máquina virtual debe tener la versión de hardware 18 o una posterior.
- La máquina virtual debe tener marcada la opción **Reservar toda la memoria de invitado**; de lo contrario, se producirá un error de encendido.
- Compruebe que la máquina virtual esté apagada.

Procedimiento

1 Conéctese a vCenter Server mediante vSphere Client.

2 Haga clic con el botón derecho en la máquina virtual en el inventario que desee modificar y seleccione **Editar configuración**.

3 En **Opciones de máquina virtual > Opciones de arranque > Firmware**, asegúrese de que EFI está seleccionado.

4 En el cuadro de diálogo **Editar configuración**, en **Opciones de máquina virtual > Cifrado**, seleccione la casilla de verificación **Habilitar** para SEV-ES de AMD.

5 Haga clic en **Aceptar**.

Resultados

Se agregó SEV-ES a la máquina virtual.

Activar el estado cifrado de SEV (Secure Encrypted Virtualization) de AMD en una máquina virtual existente mediante la línea de comandos

Puede usar la línea de comandos para agregar el estado cifrado de SEV (Secure Encrypted Virtualization-Encrypted State, SEV-ES) a una máquina virtual existente para proporcionar mayor seguridad al sistema operativo invitado.

Puede agregar el estado cifrado de SEV (Secure Encrypted Virtualization-Encrypted State, SEV-ES) a las máquinas virtuales que se ejecutan en ESXi 7.0 Update 1 o posterior.

Requisitos previos

- El sistema se debe instalar con una CPU AMD EPYC 7xx2 (código denominado "Roma") o una versión posterior y una BIOS compatible.
- El estado cifrado de SEV (Secure Encrypted Virtualization-Encrypted State, SEV-ES) debe estar activado en la BIOS.
- La BIOS controla el número de máquinas virtuales de SEV-ES por host ESXi. Al hacerlo, introduzca un valor para la opción de **ASID mínimo de estado no cifrado de SEV** que sea igual a la cantidad de máquinas virtuales con SEV-ES más una. Por ejemplo, si tiene 12 máquinas virtuales que desee ejecutar de forma simultánea, introduzca `13`.

  Nota vSphere 7.0 Update 1 y versiones posteriores admiten 16 máquinas virtuales activadas para SEV-ES por host ESXi. Si se utiliza una configuración más alta en la BIOS, SEV-ES seguirá funcionando, pero se aplica el límite de 16. vSphere 7.0 Update 2 y posteriores admiten 480 máquinas virtuales activadas para SEV-ES por host ESXi.

- El host ESXi que se ejecuta en el entorno debe ser ESXi 7.0 Update 1 o una versión posterior.
- El sistema operativo invitado debe ser compatible con el estado cifrado de SEV (Secure Encrypted Virtualization-Encrypted State, SEV-ES).

  Actualmente, solo se admiten kernels de Linux con soporte específico para el estado cifrado de SEV (Secure Encrypted Virtualization-Encrypted State, SEV-ES).
- La máquina virtual debe tener la versión de hardware 18 o una posterior.
- La máquina virtual debe tener marcada la opción **Reservar toda la memoria de invitado**; de lo contrario, se producirá un error de encendido.
- PowerCLI 12.1.0 o una versión posterior debe estar instalada en un sistema con acceso a su entorno.
- Compruebe que la máquina virtual esté apagada.

Procedimiento

1 En una sesión de PowerCLI, ejecute el cmdlet `Connect-VIServer` para conectarse como administrador a la instancia de vCenter Server que administra el host ESXi con la máquina virtual a la que desea agregar SEV-ES.

  Por ejemplo:

```
Connect-VIServer -server vCenter_Server_ip_address -User admin_user -Password 'password'
```

2 Agregue SEV-ES a la máquina virtual con el cmdlet `Set-VM`, especificando `-SEVEnabled $true`.

   Por ejemplo:

```
$vmhost = Get-VMHost -Name 10.193.25.83
Set-VM -Name MyVM2 $vmhost -SEVEnabled $true
```

   Si debe especificar la versión del hardware virtual, ejecute el cmdlet `Set-VM` con el parámetro `-HardwareVersion vmx-18`. Por ejemplo:

```
Set-VM -Name MyVM2 $vmhost -SEVEnabled $true -HardwareVersion vmx-18
```

Resultados

Se agregó SEV-ES a la máquina virtual.

Desactivar el estado cifrado de SEV (Secure Encrypted Virtualization) de AMD en una máquina virtual mediante vSphere Client

En vSphere 7.0 Update 2 y versiones posteriores, es posible utilizar vSphere Client para desactivar SEV-ES en una máquina virtual.

Requisitos previos

- Compruebe que la máquina virtual esté apagada.

Procedimiento

1 Conéctese a vCenter Server mediante vSphere Client.

2 Haga clic con el botón derecho en la máquina virtual en el inventario que desee modificar y seleccione **Editar configuración**.

3 En el cuadro de diálogo **Editar configuración**, en **Opciones de máquina virtual > Cifrado**, anule la selección de la casilla de verificación **Habilitar** para SEV-ES de AMD.

4 Haga clic en **Aceptar**.

Resultados

SEV-ES está desactivado en la máquina virtual.

Desactivar el estado cifrado de SEV (Secure Encrypted Virtualization) de AMD en una máquina virtual mediante la línea de comandos

Puede utilizar la línea de comandos para desactivar SEV-ES en una máquina virtual .

Requisitos previos

- Compruebe que la máquina virtual esté apagada.

- PowerCLI 12.1.0 o una versión posterior debe estar instalada en un sistema que tenga acceso a su entorno.

Procedimiento

1 En una sesión de PowerCLI, ejecute el cmdlet `Connect-VIServer` para conectarse como administrador a la instancia de vCenter Server que administra el host ESXi con la máquina virtual desde la que desea eliminar SEV-ES.

   Por ejemplo:

```
Connect-VIServer -server vCenter_Server_ip_address -User admin_user -Password 'password'
```

2 Desactive SEV-ES en la máquina virtual con el cmdlet `Set-VM`; para ello, especifique `-SEVEnabled $false`.

   Por ejemplo, asigne primero la información del host a una variable y, a continuación, desactive SEV-ES para la máquina virtual.

```
$vmhost = Get-VMHost -Name 10.193.25.83
Set-VM -Name MyVM2 $vmhost -SEVEnabled $false
```

Resultados

SEV-ES está desactivado en la máquina virtual.

Cifrado de máquinas virtuales

6

Con el cifrado de máquinas virtuales de vSphere, puede cifrar las cargas de trabajo confidenciales de una forma aún más segura. El acceso a las claves de cifrado puede supeditarse a que el host ESXi se encuentre en un estado de confianza.

Antes de comenzar con las tareas de cifrado de máquinas virtuales, debe configurar un proveedor de claves. Los siguientes tipos de proveedor de claves están disponibles.

Tabla 6-1. Proveedores de claves de vSphere

Proveedor de claves	Descripción	Para obtener más información
Proveedor de claves estándar	Disponible en vSphere 6.5 y versiones posteriores, el proveedor de claves estándar utiliza vCenter Server para solicitar claves a un servidor de claves externo. El servidor de claves genera y almacena las claves, y después las envía a vCenter Server para su distribución.	Consulte Capítulo 7 Configurar y administrar un proveedor de claves estándar.
Proveedor de claves de confianza	Disponible en vSphere 7.0 y versiones posteriores, el proveedor de claves de confianza vSphere Trust Authority hace que el acceso a las claves de cifrado dependa del estado de atestación de un clúster de carga de trabajo. vSphere Trust Authority requiere un servidor de claves externo.	Consulte Capítulo 9 vSphere Trust Authority.
VMware vSphere® Native Key Provider™	Disponible en vSphere 7.0 Update 2 y versiones posteriores, vSphere Native Key Provider se incluye en todas las ediciones de vSphere y no requiere un servidor de claves externo.	Consulte Capítulo 8 Configurar y administrar el proveedor de claves nativo de vSphere.

Lea los siguientes temas a continuación:

- Flujo del proceso de cifrado
- Cifrado de disco virtual
- Errores de cifrado de máquinas virtuales
- Requisitos previos y privilegios necesarios para tareas de cifrado de máquinas virtuales
- Qué es vSphere vMotion cifrado
- Prácticas recomendadas de cifrado de máquinas virtuales
- Advertencias de cifrado de máquinas virtuales
- Interoperabilidad del cifrado de máquinas virtuales
- Persistencia de claves de vSphere en hosts ESXi

Comparación de proveedores de claves de vSphere

Para obtener una descripción general de alto nivel de las capacidades de los proveedores de claves de vSphere, se requiere su atención para ayudar a planificar la estrategia de cifrado.

En general, hay poca diferencia en la compatibilidad de características o productos entre el funcionamiento diario del proveedor de claves. A pesar de que los proveedores de claves tienen una apariencia y comportamiento similares, es posible que tenga en cuenta los requisitos y las normas al elegir un proveedor de claves, como se muestra en la siguiente tabla.

Tabla 6-2. Consideraciones del proveedor de claves

Proveedor de claves	¿Se requiere el servidor de claves externo?	¿Configuración rápida?	¿Funciona solo con vSphere?	¿Claves de cifrado almacenadas permanentemente en el host?	¿Regenerar clave durante la clonación?
Proveedor de claves estándar	Sí	No	No	No	Sí
Proveedor de claves de confianza	Sí	No	No	No	Sí
vSphere Native Key Provider	No	Sí	Sí	Sí	Sí

Nota Al iniciar el host, vSphere Native Key Provider siempre escribe la clave de cifrado en los hosts de ESXi del clúster. Si le preocupa la seguridad física del clúster, considere la posibilidad de utilizar un proveedor de claves estándar o uno de confianza; ambos requieren que el servidor de claves esté disponible para que las máquinas virtuales cifradas funcionen.

Funciones de cifrado del proveedor de claves

Las siguientes funciones de cifrado son compatibles con cada tipo de proveedor de claves.

- Vuelva a crear claves con el mismo proveedor de claves o con otro.
- Rote las claves
- Módulo de plataforma de confianza virtual (Virtual Trusted Platform Module, vTPM)
- Cifrado de discos
- Cifrado de máquinas virtuales de vSphere
- Coexistencia con otros proveedores de claves
- Actualizar a otro proveedor de claves

Compatibilidad del proveedor de claves con funciones de vSphere

A continuación, se describen las funciones importantes que se admiten en el proveedor de claves de vSphere.

- vSphere vMotion encriptadas: compatibles con todos los tipos de proveedores de claves. El mismo proveedor de claves debe estar disponible en el host de destino. Consulte Qué es vSphere vMotion cifrado.
- Copia de seguridad y restauración basada en archivos de vCenter Server: el proveedor de claves estándar y vSphere Native Key Provider admiten vCenter Server copia de seguridad y restauración basada en archivos. Debido a que la mayor parte de la información de configuración de vSphere Trust Authority se almacena en los hosts ESXi, el mecanismo de copia de seguridad basada en archivo vCenter Server no hace la copia de seguridad de esta información. de . Para garantizar que se hayan guardado los datos de configuración de la implementación de vSphere Trust Authority, consulte Realizar una copia de seguridad de la configuración de vSphere Trust Authority.

Soporte de proveedores de claves para productos VMware

En la siguiente tabla, se compara la compatibilidad del proveedor de claves con algunos productos VMware.

Tabla 6-3. Comparación de la compatibilidad con productos VMware

Proveedor de claves	Cifrado de datos en reposo de vSAN	Site Recovery Manager	vSphere Replication
Proveedor de claves estándar	Sí	Sí	Sí
Proveedor de claves de confianza	No	Sí Si la misma configuración de servicios vSphere Trust Authority está disponible en el lado de la recuperación, se admite SRM con replicación basada en matrices.	No
vSphere Native Key Provider	Sí	Sí	Sí

Nota El proveedor de claves estándar, el proveedor de claves de confianza y vSphere Native Key Provider admiten el cifrado de máquinas virtuales de vSphere sobre vSAN.

Hardware requerido para proveedores de claves

En la siguiente tabla se comparan algunos requisitos mínimos de hardware del proveedor de claves.

Tabla 6-4. Comparación del hardware requerido para los proveedores de claves

Proveedor de claves	TPM en host ESXi
Proveedor de claves estándar	No son obligatorias
Proveedor de claves de confianza	Se requiere en hosts de confianza (hosts en el clúster de confianza). **Nota** Actualmente, los hosts ESXi del clúster de Trust Authority no requieren un TPM. Sin embargo, como práctica recomendada, considere la posibilidad de instalar nuevos hosts ESXi con TPM.
vSphere Native Key Provider	No son obligatorias La disponibilidad de vSphere Native Key Provider puede limitarse opcionalmente a los hosts con un TPM.

Nomenclatura de proveedor de claves

vSphere utiliza un nombre de proveedor de claves para buscar un identificador de clave. Si dos proveedores de claves tienen el mismo nombre, vSphere asume que son equivalentes y tienen acceso a las mismas claves. Cada proveedor de claves lógico, independientemente de su tipo (proveedor de claves estándar, de confianza y nativo), debe tener un nombre único en todos los sistemas vCenter Server.

En unos pocos casos, se puede configurar el mismo proveedor de claves en varios sistemas vCenter Server, como:

- Migrar máquinas virtuales cifradas entre sistemas vCenter Server.
- Configurar una instancia de vCenter Server como sitio de recuperación ante desastres.

Cómo el cifrado de máquinas virtuales de vSphere protege el entorno

Independientemente del proveedor de claves que utilice, con cifrado de máquinas virtuales de vSphere puede crear máquinas virtuales cifradas y cifrar máquinas virtuales existentes. Debido a que se cifran todos los archivos de máquinas virtuales con información confidencial, la máquina virtual está protegida. Solo los administradores con privilegios de cifrado puede realizar tareas de cifrado y descifrado.

Importante Los usuarios de ESXi Shell también tienen privilegios de operaciones criptográficas. Para obtener más información, consulte Requisitos previos y privilegios necesarios para tareas de cifrado de máquinas virtuales.

Qué almacenamiento admite el cifrado de máquinas virtuales de vSphere

El cifrado de máquinas virtuales de vSphere funciona con cualquier tipo de almacenamiento compatible (NFS, iSCSI, canal de fibra, etc.), incluido VMware vSAN. Para obtener más información sobre el uso del cifrado en un clúster de vSAN, consulte la documentación de *Administrar VMware vSAN*.

El cifrado de máquinas virtuales de vSphere y vSAN utilizan las mismas bibliotecas de cifrado, pero tienen perfiles diferentes. El cifrado de máquina virtual corresponde a un cifrado por máquina virtual y vSAN es un cifrado de nivel de almacén de datos.

Claves de cifrado y proveedores de claves de vSphere

vSphere utiliza dos niveles de cifrado en forma de una clave de cifrado de claves (Key Encryption Key, KEK) y una clave de cifrado de datos (Data Encryption Key, DEK). En pocas palabras, un host ESXi genera una DEK para cifrar máquinas virtuales y discos. Un servidor de claves proporciona la KEK y cifra (o "encapsula") la DEK. KEK cifra la DEK mediante el algoritmo AES256 y la DEK cifra el VMDK mediante el algoritmo XTS-AES-256 (tamaño de la clave de 512 bits). En función del tipo de proveedor de claves, se utilizan diferentes métodos para crear y administrar la DEK y la KEK.

El proveedor de claves estándar funciona de la siguiente manera.

1 El host ESXi genera y usa claves internas para cifrar máquinas y discos virtuales. Estas claves se utilizan como DEK.

2 vCenter Server Solicitudes de claves del servidor de claves (KMS). Estas claves se utilizan como KEK. vCenter Server almacena solo el identificador de cada KEK, pero no la clave en sí.

3 ESXi utiliza la KEK para cifrar las claves internas y almacena la clave interna cifrada en el disco. ESXi no almacena la KEK en el disco. Si un host se reinicia, vCenter Server solicita la KEK con el identificador correspondiente del servidor de claves y la pone a disposición de ESXi. De este modo, ESXi puede descifrar las claves internas según sea necesario.

El proveedor de claves de confianza vSphere Trust Authority funciona de la siguiente manera.

1 La instancia de vCenter Server del clúster de confianza comprueba si el proveedor de claves de confianza predeterminado está accesible para el host ESXi en el que se va a crear la máquina virtual cifrada.

2 La instancia de vCenter Server del clúster de confianza agrega el proveedor de claves de confianza a la máquina virtual ConfigSpec.

3 La solicitud de creación de la máquina virtual se envía al host ESXi.

4 Si no hay un token de atestación disponible para el host ESXi, solicita uno al servicio de atestación.

5 El servicio de proveedor de claves valida el token de atestación y crea una clave de cifrado de claves que se enviará al host ESXi. La KEK está envuelta (cifrada) con la clave principal que está configurada en el proveedor de claves. El texto cifrado y el texto sin formato de la KEK se devuelven al host de confianza.

6 El host ESXi genera una DEK para cifrar los discos de máquina virtual.

7 La KEK se utiliza para envolver las DEK que genera el host ESXi, y el texto cifrado del proveedor de claves se almacena junto con los datos cifrados.

8 La máquina virtual está cifrada y se escribe en el almacenamiento.

Nota Los hosts ESXi en los clústeres de vSphere contienen la KEK para máquinas virtuales cifradas en la memoria de host a fin de habilitar las funciones de disponibilidad, como Alta disponibilidad, vMotion, DRS, etc. Cuando se elimina o se cancela el registro de una máquina virtual, los hosts ESXi del clúster eliminan la KEK de su memoria. De este modo, los hosts ESXi ya no pueden utilizar la KEK. Este comportamiento es el mismo para los proveedores de claves estándar y los proveedores de claves de confianza.

---

vSphere Native Key Provider funciona de la siguiente manera.

1 Cuando se crea el proveedor de claves, vCenter Server genera una clave principal y la inserta en ESXi hosts del clúster. (No hay ningún servidor de claves externo implicado).

2 Los hosts ESXi generan una DEK a petición.

3 Cuando se realiza una actividad de cifrado, los datos se cifran con la DEK.

Las DEK cifradas se almacenan junto con los datos cifrados.

4 Al descifrar datos, se utiliza la clave principal para descifrar la DEK y, a continuación, los datos.

Qué componentes se cifran con el cifrado de máquinas virtuales de vSphere

El cifrado de máquinas virtuales de vSphere admite el cifrado de archivos de máquinas virtuales, archivos de discos virtuales y archivos de volcados de núcleo.

Archivos de la máquina virtual

Se cifra la mayoría de los archivos de máquinas virtuales, en particular los datos de invitados que no se almacenan en el archivo VMDK. Este conjunto de archivos incluye, entre otros, los archivos de NVRAM, VSWP y VMSN. La clave que del proveedor de claves desbloquea un paquete cifrado en el archivo VMX que contiene claves internas y otros secretos. La recuperación de claves funciona de la siguiente manera, según el proveedor de claves:

- Proveedor de claves estándar: vCenter Server administra las claves desde el servidor de claves y los hosts ESXi no pueden acceder directamente al proveedor de claves. Los hosts esperan a vCenter Server para insertar las claves.
- Proveedor de claves de confianza y vSphere Native Key Provider: los hosts ESXi acceden directamente a los proveedores de claves y, por lo tanto, recupera las claves solicitadas directamente desde el servicio de vSphere Trust Authority o desde la instancia de vSphere Native Key Provider.

Cuando se utiliza vSphere Client para crear una máquina virtual cifrada, puede cifrar y descifrar discos virtuales de manera independiente de archivos de máquinas virtuales. Todos los discos virtuales están cifrados de forma predeterminada. Para otras tareas de cifrado, como el cifrado de una máquina virtual existente, puede cifrar y descifrar discos virtuales de manera independiente de los archivos de máquinas virtuales.

Nota No se puede asociar un disco virtual cifrado con una máquina virtual que no está cifrada.

Archivos de disco virtual

Los datos de un archivo de disco virtual cifrado (VMDK) jamás se escriben en texto no cifrado en el almacenamiento o el disco físico, ni tampoco se transmiten por la red en texto no cifrado. El archivo de descriptor de VMDK incluye en su mayoría texto no cifrado, pero contiene un identificador de clave para la KEK y la clave interna (DEK) en el paquete cifrado.

Puede utilizar vSphere Client o la vSphere API para realizar una operación de repetición de cifrado superficial con una nueva KEK o utilizar la vSphere API para realizar una operación de repetición de cifrado profunda con una nueva clave interna.

Volcados de núcleos

Los volcados de núcleo en un host ESXi en el que se habilitó el modo de cifrado siempre están cifrados. Consulte Cifrado de máquinas virtuales de vSphere y volcados de núcleo. Los volcados de núcleo en el sistema vCenter Server no están cifrados. Proteja el acceso al sistema vCenter Server.

Archivo de intercambio de la máquina virtual

El archivo de intercambio de la máquina virtual se cifra cada vez que se agrega un vTPM a una máquina virtual. Los entornos con poca memoria RAM pueden experimentar paginación relacionada con el cifrado que podría afectar el rendimiento.

vTPM

Al configurar un vTPM, se cifran los archivos de la máquina virtual, pero no los discos. Puede optar por agregar cifrado de forma explícita para la máquina virtual y sus discos. Para obtener más información, consulte Capítulo 11 Proteger las máquinas virtuales con el módulo de plataforma de confianza virtual.

Nota Para obtener información sobre algunas limitaciones relacionadas con dispositivos y características con las que puede interoperar el cifrado de máquinas virtuales de vSphere, consulte Interoperabilidad del cifrado de máquinas virtuales.

Qué componentes no se cifran con el cifrado de máquinas virtuales de vSphere

Algunos de los archivos relacionados con una máquina virtual no se cifran o se cifran parcialmente.

Archivos de registro

Los archivos de registro no se cifran, ya que no contienen datos confidenciales.

Archivos de configuración de máquinas virtuales

La mayoría de la información de configuración de máquinas virtuales, almacenada en los archivos VMX y VMSD, no está cifrada.

Archivo de descriptor de discos virtuales

Para admitir la administración de discos sin una clave, la mayor parte del archivo de descriptor de discos virtuales no se cifra.

Qué privilegios son necesarios para realizar operaciones criptográficas

Solo los usuarios a los que se asignan privilegios de **Operaciones criptográficas** pueden realizar operaciones criptográficas. El conjunto de privilegios tiene una granularidad fina. La función del sistema predeterminada Administrador incluye todos los privilegios de **Operaciones criptográficas**. La función Sin administrador de criptografía admite todos los privilegios de Administrador, salvo los privilegios de **Operaciones criptográficas**.

Además de usar el **Criptógrafo.***, privilegios, vSphere Native Key Provider puede utilizar el privilegio **Cryptographer.ReadKeyServersInfo**, que es específico de las instancias de vSphere Native Key Provider.

Consulte Privilegios de operaciones de cifrado para obtener más información.

Puede crear funciones personalizadas adicionales, por ejemplo, para permitir que un grupo de usuarios cifre máquinas virtuales, pero impedirles que las descifren.

Cómo realizar operaciones criptográficas

vSphere Client admite muchas de las operaciones criptográficas. Para otras tareas, puede usar PowerCLI o la vSphere API.

Tabla 6-5. Interfaces para realizar operaciones criptográficas

Interfaz	Operaciones	Información
vSphere Client	Crear una máquina virtual cifrada Cifrar y descifrar máquinas virtuales Realice una operación de repetición de cifrado superficial de una máquina virtual (con otra KEK).	Este libro.
PowerCLI	Crear una máquina virtual cifrada Cifrar y descifrar máquinas virtuales Configuración de vSphere Trust Authority	*Referencia de cmdlets VMware PowerCLI*
vSphere Web Services SDK	Crear una máquina virtual cifrada Cifrar y descifrar máquinas virtuales Realice una operación de repetición de cifrado profunda de una máquina virtual (con otra DEK). Realice una operación de repetición de cifrado superficial de una máquina virtual (con otra KEK).	*Guía de programación de vSphere Web Services SDK* *Referencia de vSphere Web Services API*
`crypto-util`	Descifrar volcados de núcleo cifrados Comprobar si los archivos están cifrados Realizar otras tareas de administración directamente en el host ESXi	Ayuda de línea de comandos. Cifrado de máquinas virtuales de vSphere y volcados de núcleo

Cómo volver a cifrar (regenerar claves) una máquina virtual cifrada

Puede repetir el cifrado (o también regenerar clave) de una máquina virtual con nuevas claves, por ejemplo, en caso de que una clave caduque o se ponga en riesgo la seguridad. Están disponibles las siguientes opciones de recodificación.

- Una recodificación superficial, que sustituye solo la clave de cifrado de claves (KEK)
- Una recodificación profunda, que sustituye tanto la clave de cifrado de disco (DEK) como la KEK

Para una repetición de cifrado profunda, es necesario que la máquina virtual esté desconectada y no contenga instantáneas. Puede realizar una operación de repetición de cifrado superficial mientras la máquina virtual esté encendida y si esta contiene instantáneas. La repetición de cifrado superficial de una máquina virtual cifrada con instantáneas solo se permite en una única rama de instantáneas (cadena de discos). No se admiten varias ramas de instantáneas. Además, no se admite repetición de cifrado superficial en un clon vinculado de una máquina virtual o un disco. Si se produce un error en la repetición de cifrado superficial antes de actualizar todos los vínculos de la cadena con la nueva KEK, aún se puede acceder a la máquina virtual cifrada si tiene la KEK antigua y la nueva. Sin embargo, lo mejor es volver a ejecutar la operación de repetición de cifrado superficial antes de realizar operaciones de instantáneas.

Puede regenerar una clave de una máquina virtual mediante vSphere Client, la CLI o la API. Consulte Cambiar la clave de una máquina virtual cifrada mediante vSphere Client, Regenerar claves de una máquina virtual cifrada mediante la CLI y *Guía de programación de vSphere Web Services SDK*.

Componentes de cifrado de máquinas virtuales de vSphere

Según el proveedor de claves que utilice, un servidor de claves externo, el sistema vCenter Server y los hosts ESXi contribuyen potencialmente a la solución de cifrado.

Los siguientes componentes incluyen el cifrado de máquinas virtuales de vSphere:

- Un servidor de claves externo, también denominado KMS (no es necesario para vSphere Native Key Provider)
- vCenter Server
- Hosts de ESXi

Cuál es la función de un servidor de claves en el cifrado de máquinas virtuales de vSphere

El servidor de claves es un servidor de administración del protocolo de interoperabilidad de administración de claves (Key Management Interoperability Protocol, KMIP) que está asociado con un proveedor de claves. Un proveedor de claves estándar y un proveedor de claves de confianza requieren un servidor de claves. vSphere Native Key Provider no requiere un servidor de claves. En la siguiente tabla se describen las diferencias en la interacción entre el proveedor de claves y el servidor de claves.

Tabla 6-6. Interacción entre los proveedores de claves y el servidor de claves

Proveedor de claves	Interacción con el servidor de claves
Proveedor de claves estándar	Un proveedor de claves estándar utiliza vCenter Server para solicitar claves de un servidor de claves. El servidor de claves genera y almacena las claves, y después las envía a vCenter Server para su distribución a los hosts ESXi.
Proveedor de claves de confianza	Un proveedor de claves de confianza utiliza un servicio de proveedor de claves que permite a los hosts ESXi de confianza recuperar las claves directamente. Consulte Descripción del servicio de proveedor de claves de vSphere Trust Authority.
Proveedor de claves nativo de vSphere	vSphere Native Key Provider no requiere un servidor de claves. vCenter Server genera una clave principal y la inserta en los hosts ESXi. Luego, los hosts ESXi generan claves de cifrado de datos (incluso cuando no están conectados a vCenter Server). Consulte Descripción general de vSphere Native Key Provider.

Puede utilizar vSphere Client o vSphere API para agregar instancias de proveedor de claves al sistema de vCenter Server. Si utiliza varias instancias de proveedor de claves, todas deben ser del mismo proveedor y deben replicar claves.

Si el entorno utiliza distintos proveedores de servidores de claves en diferentes entornos, puede agregar un proveedor de claves para cada servidor de claves y especificar un proveedor de claves predeterminado. El primer proveedor de claves que agregue será el predeterminado. Podrá especificar explícitamente el predeterminado más adelante.

Como cliente de KMIP, vCenter Server utiliza un protocolo de interoperabilidad de administración de claves (Key Management Interoperability Protocol, KMIP) para que sea sencillo utilizar el servidor de claves que el usuario desea.

Cuál es la función de vCenter Serveren el cifrado de máquinas virtuales de vSphere

En la siguiente tabla se describe la función de las instancias de vCenter Server en el proceso de cifrado.

Tabla 6-7. Proveedores de claves y vCenter Server

Proveedor de claves	Función de vCenter Server	Cómo se comprueban los privilegios
Proveedor de claves estándar	Solo vCenter Server tiene credenciales para iniciar sesión en el servidor de claves. Los hosts ESXi no tienen esas credenciales. vCenter Server obtiene las claves del servidor de claves y las inserta en los hosts ESXi. vCenter Server no almacena las claves del servidor de claves, pero sí conserva una lista de identificadores de claves.	vCenter Server comprueba los privilegios de los usuarios que realizan operaciones criptográficas.
Proveedor de claves de confianza	vSphere Trust Authority elimina la necesidad de que vCenter Server solicite claves al servidor de claves y hace que el acceso a las claves de cifrado dependa del estado de atestación de un clúster de carga de trabajo. Debe utilizar sistemas vCenter Server independientes para el clúster de confianza y el clúster de Trust Authority.	vCenter Server comprueba los privilegios de los usuarios que realizan operaciones criptográficas. Solo los usuarios que son miembros del grupo de SSO TrustedAdmins pueden realizar operaciones administrativas.
Proveedor de claves nativo de vSphere	vCenter Server genera las claves.	vCenter Server comprueba los privilegios de los usuarios que realizan operaciones criptográficas.

Puede utilizar vSphere Client para asignar privilegios de operaciones criptográficas o para asignar la función personalizada **Sin administrador de criptografía** a grupos de usuarios. Consulte Requisitos previos y privilegios necesarios para tareas de cifrado de máquinas virtuales.

vCenter Server agrega eventos de cifrado a la lista de eventos que se pueden ver y exportar de la consola de eventos de vSphere Client. Cada evento incluye el usuario, la hora, el identificador de clave y la operación criptográfica.

Las claves que provienen del servidor de claves se utilizan como claves de cifrado de claves (key encryption key, KEK).

Cuál es la función de los hosts ESXi en el cifrado de máquinas virtuales de vSphere

Los hosts ESXi se encargan de diversos aspectos del flujo de trabajo de cifrado.

Tabla 6-8. Proveedores de claves y hosts ESXi

Proveedor de claves	Aspectos de los hosts ESXi
Proveedor de claves estándar	■ vCenter Server introduce claves en un host ESXi cuando el host necesita una clave. El host debe tener habilitado el modo de cifrado. ■ Garantizar que los datos del invitado de las máquinas virtuales cifradas estén cifrados cuando se almacenan en el disco. ■ Garantizar que los datos del invitado de las máquinas virtuales cifradas no se envíen a la red sin cifrar.
Proveedor de claves de confianza	Los hosts ESXi ejecutan servicios de vSphere Trust Authority, en función de si son hosts de confianza o hosts de Trust Authority. Los hosts ESXi de confianza ejecutan máquinas virtuales de carga de trabajo que se pueden cifrar mediante proveedores de claves publicados por los hosts de Trust Authority. Consulte Infraestructura de confianza de vSphere Trust Authority.
Proveedor de claves nativo de vSphere	Los hosts ESXi recuperan claves directamente de vSphere Native Key Provider.

Las claves que generan los hosts ESXi se denominan claves internas en este documento. Estas claves, por lo general, actúan como claves de cifrado de datos (Data Encryption Key, DEK).

Flujo del proceso de cifrado

Después de que configura un proveedor de claves, los usuarios que tengan los privilegios necesarios pueden crear máquinas y discos virtuales cifrados. Esos usuarios también pueden cifrar máquinas virtuales existentes y descifrar máquinas virtuales cifradas y agregar módulos de plataforma de confianza virtual (vTPM) a las máquinas virtuales.

Según el tipo de proveedor de claves, el flujo del proceso puede incluir un servidor de claves, el vCenter Server y el ESXi host.

Flujo del proceso de cifrado del proveedor de claves estándar

Durante el proceso de cifrado, los distintos componentes de vSphere interactúan del siguiente modo.

1 Cuando el usuario realiza una tarea de cifrado, por ejemplo, crear una máquina virtual cifrada, vCenter Server solicita una nueva clave del servidor de claves predeterminado. Esta clave se utiliza como la KEK.

2 vCenter Server almacena el identificador de la clave y pasa la clave al host ESXi. Si el host ESXi es parte del clúster, vCenter Server envía la KEK a cada host del clúster.

   La clave en sí no se guarda en el sistema de vCenter Server. Solo se conoce el identificador de la clave.

3 El host ESXi genera claves internas (DEK) para la máquina virtual y sus discos. Mantiene las claves internas solo en la memoria y usa las KEK para cifrar las claves internas.

   Nunca se guardan en el disco las claves internas sin cifrar. Solo se guardan los datos cifrados. Dado que las KEK provienen del servidor de claves, el host sigue usando las mismas KEK.

4 El host ESXi cifra la máquina virtual con la clave interna cifrada.

   Todos los hosts que tengan la KEK y puedan acceder al archivo de la clave cifrada pueden realizar operaciones en la máquina o el disco virtual cifrado.

Flujo del proceso de cifrado del proveedor de claves de confianza

El flujo del proceso de cifrado de vSphere Trust Authority incluye los servicios de vSphere Trust Authority, los proveedores de claves de confianza, la instancia de vCenter Server y los hosts ESXi.

El cifrado de una máquina virtual con un proveedor de claves de confianza tiene el mismo aspecto que la experiencia del usuario de cifrado de máquinas virtuales cuando se utiliza un proveedor de claves estándar. El cifrado de máquinas virtuales en vSphere Trust Authority sigue dependiendo de las directivas de almacenamiento de cifrado de máquinas virtuales o de la presencia de un dispositivo vTPM, para decidir cuándo cifrar una máquina virtual. Aún puede utilizar un proveedor de claves configurado de forma predeterminada (denominado clúster KMS en vSphere 6.5 y 6.7) cuando cifre una máquina virtual desde vSphere Client. También puede utilizar las API de una manera similar para especificar el proveedor de claves manualmente. Los privilegios de cifrado existentes agregados para vSphere 6.5 siguen aplicándose en vSphere 7.0 y versiones posteriores para vSphere Trust Authority.

El proceso de cifrado del proveedor de claves de confianza tiene algunas diferencias importantes con respecto al proveedor de claves estándar:

- Los administradores de Trust Authority no especifican información directamente al configurar un servidor de claves para una instancia de vCenter Server y no establecen la confianza de servidor de claves. En su lugar, vSphere Trust Authority publica proveedores de claves de confianza que los hosts de confianza pueden utilizar.
- vCenter Server ya no inserta claves para hosts ESXi y, en su lugar, puede tratar a cada proveedor de claves de confianza como una sola clave de nivel superior.
- Solo los hosts de confianza pueden solicitar operaciones de cifrado desde hosts de Trust Authority.

Flujo del proceso de cifrado de vSphere Native Key Provider

vSphere Native Key Provider se incluye en vSphere 7.0 Update 2 y versiones posteriores. Al configurar una instancia de vSphere Native Key Provider, vCenter Server inserta una clave principal en todos ESXi hosts del clúster. Del mismo modo, si actualiza o elimina una instancia de vSphere Native Key Provider, el cambio se inserta en los hosts del clúster. El flujo del proceso de cifrado es similar al funcionamiento de un proveedor de claves de confianza. La diferencia es que vSphere Native Key Provider genera las claves y las encapsula con la clave principal y, a continuación, las entrega de vuelta para realizar el cifrado.

Atributos personalizados para servidores de claves

El protocolo de interoperabilidad para la administración de claves (Key Management Interoperability Protocol, KMIP) admite la adición de atributos personalizados destinados a propósitos específicos de cada proveedor. Los atributos personalizados permiten identificar más específicamente las claves almacenadas en el servidor de claves. vCenter Server agrega los siguientes atributos personalizados para claves de máquina virtual y claves de host.

Tabla 6-9. Atributos personalizados de cifrado de máquinas virtuales

Atributo personalizado	Valor
`x-Vendor`	VMware, Inc.
`x-Product`	VMware vSphere
`x-Product_Version`	Versión de vCenter Server
`x-Component`	Máquina virtual
`x-Name`	Nombre de la máquina virtual (que se recopila de ConfigInfo o ConfigSpec)
`x-Identifier`	UUID de instancia de la máquina virtual (que se recopila de ConfigInfo o ConfigSpec)

Tabla 6-10. Atributos personalizados de cifrado de host

Atributo personalizado	Valor
`x-Vendor`	VMware, Inc.
`x-Product`	VMware vSphere
`x-Product_Version`	Versión de vCenter Server
`x-Component`	Servidor ESXi
`x-Name`	Nombre de host
`x-Identifier`	UUID de hardware del host

vCenter Server agrega los atributos `x-Vendor`, `x-Product` y `x-Product_Version` cuando el servidor de claves crea una clave. Cuando se utiliza la clave para cifrar una máquina virtual o un host, vCenter Server establece los atributos `x-Component`, `x-Identifier` y `x-Name`. Es posible que pueda ver estos atributos personalizados en la interfaz de usuario del servidor de claves. Consulte con su proveedor de servidores de claves.

Tanto la clave de host como la clave de máquina virtual tienen los seis atributos personalizados. `x-Vendor`, `x-Product` y `x-Product_Version` pueden ser los mismos para ambas claves. Estos atributos se establecen cuando se genera la clave. Dependiendo de si la clave es para una máquina virtual o un host, es posible que se hayan anexado los atributos `x-Component`, `x-Identifier` y `x-Name`.

Errores de claves de cifrado

Cuando se produce un error al enviar claves del servidor de claves a un host ESXi, vCenter Server genera un mensaje en el registro de eventos para los siguientes eventos:

- Error al agregar claves al host ESXi debido a problemas de conexión o compatibilidad del host.
- Se produjo un error al obtener claves del servidor de claves debido a que faltaba una clave en el servidor de claves.
- No se pudieron obtener las claves del servidor de claves debido a la conexión del servidor de claves.

Descifrar máquinas virtuales cifradas

Si posteriormente desea descifrar una máquina virtual cifrada, puede cambiar su directiva de almacenamiento. Puede cambiar la directiva de almacenamiento de la máquina virtual y todos los discos. Si desea descifrar un componente individual, descifre primero el componente seleccionado y luego descifre la máquina virtual cambiando la directiva de almacenamiento para el inicio de la máquina virtual. Ambas claves son necesarias para descifrar cada uno de los componentes. Consulte Descifrar una máquina virtual o un disco virtual cifrados.

Cifrado de disco virtual

Cuando se crea una máquina virtual cifrada a partir de vSphere Client, puede decidir qué discos se excluirán del cifrado. Posteriormente, puede agregar discos y establecer sus directivas de cifrado. No se puede agregar un disco cifrado a una máquina virtual que no está cifrada y no se puede cifrar un disco si la máquina virtual no está cifrada.

El cifrado de una máquina virtual y de sus discos se controla mediante directivas de almacenamiento. La directiva de almacenamiento de inicio de la máquina virtual rige la propia máquina, virtual y cada disco virtual tiene una directiva de almacenamiento asociada.La directiva de almacenamiento de inicio de la máquina virtual rige la propia máquina, y cada disco virtual tiene una directiva de almacenamiento asociada.

- Al definir la directiva de almacenamiento de inicio de la máquina virtual con una directiva de cifrado, solo se cifra la máquina virtual.
- Al definir la directiva de almacenamiento de inicio de la máquina virtual y de todos los discos con una directiva de cifrado, se cifran todos los componentes.

Tenga en cuenta los siguientes casos de uso.

Tabla 6-11. Casos de uso de cifrado de discos virtuales

Caso de uso	Detalles
Cree una máquina virtual cifrada.	Si agrega discos al crear una máquina virtual cifrada, los discos se cifran de manera predeterminada. Puede cambiar la directiva de manera que no se cifren uno o más discos. Después de la creación de una máquina virtual, puede cambiar explícitamente la directiva de almacenamiento de cada disco. Consulte Cambiar la directiva de cifrado para discos virtuales.
Cifre una máquina virtual.	Para cifrar una máquina virtual actual, debe cambiar la directiva de almacenamiento.Para cifrar una máquina virtual, debe cambiar la directiva de almacenamiento. Se puede cambiar la directiva de almacenamiento de la máquina virtual y de todos los discos virtuales. Para cifrar solo la máquina virtual, puede especificar una directiva de cifrado para el inicio de la máquina virtual y seleccionar una directiva de almacenamiento diferente para cada disco virtual (por ejemplo, Valor predeterminado de almacén de datos). Consulte Crear una máquina virtual cifrada.
Agregue un disco sin cifrar existente a la máquina virtual cifrada (directiva de almacenamiento de cifrado).	Se produce un error. Debe agregar el disco con la directiva de almacenamiento predeterminada, pero luego puede cambiar la directiva de almacenamiento. Consulte Cambiar la directiva de cifrado para discos virtuales.
Agregar un disco sin cifrar actual a una máquina virtual cifrada con una directiva de almacenamiento que no incluye cifrado, por ejemplo, Valor predeterminado de almacén de datos.	El disco utiliza la directiva de almacenamiento predeterminada. Puede cambiar de manera explícita la directiva de almacenamiento después de agregar el disco si desea un disco cifrado. Consulte Cambiar la directiva de cifrado para discos virtuales.
Agregar un disco cifrado a una máquina virtual cifrada. La directiva de almacenamiento del inicio de la máquina virtual es Cifrado.	Cuando agrega el disco, este permanece cifrado. La instancia de vSphere Client muestra el tamaño y otros atributos, incluido el estado de cifrado.

Tabla 6-11. Casos de uso de cifrado de discos virtuales (continuación)

Caso de uso	Detalles
Agregar un disco cifrado existente a una máquina virtual sin cifrar.	Este caso de uso no es compatible. Sin embargo, si utiliza vSphere Client para cifrar los archivos de inicio de la máquina virtual, puede volver a configurarla sin cifrar con el disco cifrado.
Registrar una máquina virtual cifrada.	Si elimina una máquina virtual cifrada de vCenter Server, pero no la elimina del disco, puede volver a ponerla en el inventario de vCenter Server registrando el archivo de configuración de máquina virtual (.vmx) de la máquina virtual. Para registrar la máquina virtual cifrada, el usuario debe tener el privilegio **Operaciones de cifrado.Registrar máquina virtual**. Si la máquina virtual se cifró mediante un proveedor de claves estándar, cuando la máquina virtual cifrada se registre, vCenter Server envía las claves requeridas al host ESXi. Si el usuario que registra la máquina virtual no tiene el privilegio **Operaciones de cifrado.Registrar máquina virtual**, vCenter Server bloquea la máquina virtual durante el registro, y la máquina virtual no se puede usar hasta que se desbloquee. Si la máquina virtual se cifró mediante un proveedor de claves de confianza o vSphere Native Key Provider, cuando la máquina virtual cifrada se registre, vCenter Server dejará de enviar claves al host ESXi. En su lugar, las claves se recuperan del host cuando la máquina virtual se registre. Si el usuario que registra la máquina virtual no tiene el privilegio **Operaciones de cifrado.Registrar máquina virtual**, vCenter Server no permite la operación.

Errores de cifrado de máquinas virtuales

Si vCenter Server detecta un error crítico con el cifrado de máquinas virtuales, crea un evento. Puede ver estos eventos para ayudar a solucionar problemas y resolver errores de cifrado.

vCenter Server crea eventos para los siguientes errores críticos de cifrado de máquinas virtuales.

- Error al generar una KEK.
- Espacio de disco insuficiente en el almacén de datos para crear una máquina virtual cifrada.
- Privilegio de usuario insuficiente para iniciar la operación de cifrado.
- Falta la clave especificada en el proveedor de claves, por lo que la clave de host ESXi se renueva con una clave nueva.
- Se produjo un error en el proveedor de claves con la clave especificada y, por tanto, la clave de host ESXi se renueva con una clave nueva.

Requisitos previos y privilegios necesarios para tareas de cifrado de máquinas virtuales

Las tareas de cifrado de máquinas virtuales son solo posibles en los entornos que incluyen vCenter Server. Además, el host ESXi debe tener un modo de cifrado activado para la mayoría de las tareas de cifrado. El usuario que realiza la tarea debe contar con los privilegios correspondientes. Un conjunto de privilegios **Operaciones criptográficas** permite un control detallado. Si las tareas de cifrado de máquinas virtuales requieren un cambio en el modo de cifrado de host, se requieren privilegios adicionales.

Nota vSphere Trust Authority tiene requisitos previos adicionales y privilegios obligatorios. Consulte Requisitos previos y privilegios necesarios para vSphere Trust Authority.

Usar las funciones y los privilegios de cifrado

De manera predeterminada, el usuario con la función Administrador de vCenter Server tiene todos los privilegios, incluidos los privilegios para operaciones criptográficas. La función **Sin administrador de criptografía** no tiene los siguientes privilegios que se requieren para las operaciones criptográficas.

Importante Los usuarios de ESXi Shell también tienen privilegios de operaciones criptográficas.

- Agregue los privilegios **Operaciones criptográficas**.
- **Global.Diagnósticos**
- **Host.Inventario.Agregar host a clúster**
- **Host.Inventario.Agregar host independiente**
- **Host.Operaciones locales.Administrar grupos de usuarios**

Puede asignar la función **Sin administrador de criptografía** para los administradores de vCenter Server que no necesitan privilegios **Operaciones criptográficas**.

Para imponer más límites a lo que pueden hacer los usuarios, puede clonar la función **Sin administrador de criptografía** y crear una función personalizada con solo algunos privilegios **Operaciones criptográficas**. Por ejemplo, puede crear una función que permita a los usuarios cifrar máquinas virtuales, pero no descifrarlas. Consulte Usar funciones de vCenter Server para asignar privilegios.

Qué es el modo de cifrado de host

El modo de cifrado de host determina si un host ESXi está listo para aceptar material de cifrado con el fin de cifrar las máquinas virtuales y los discos virtuales. Para poder realizar cualquier operación criptográfica en un host, el modo de cifrado debe estar activado. A menudo, el modo de cifrado de host se establece automáticamente cuando es necesario, pero se puede establecer de forma explícita. Puede comprobar y establecer de forma intencional el modo de cifrado de host actual desde vSphere Client o mediante vSphere API.

Cuando se activa el modo de cifrado de host, vCenter Server instala una clave de host en el host, lo que garantiza que el host esté "seguro" desde el punto de vista del cifrado. Tras establecer la clave de host, se pueden realizar otras operaciones criptográficas, incluidas la obtención por parte de vCenter Server de claves del proveedor de claves y la inserción de estas en los hosts ESXi.

En el modo "seguro", se cifran los volcados de núcleos de los ámbitos de usuario (es decir, hostd) y las máquinas virtuales cifradas. No se cifran los volcados de núcleos de las máquinas virtuales sin cifrar.

Para obtener más información sobre los volcados de núcleos cifrados y la forma en que los utiliza el soporte técnico de VMware, consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/2147388.

Para obtener instrucciones, consulte Activar el modo de cifrado de host de forma explícita.

Una vez que se establezca el modo de cifrado de host, no podrá desactivarse con facilidad. Consulte Desactivar el modo de cifrado de host mediante la API.

Los cambios automáticos se producen cuando las operaciones de cifrado intentan establecer el modo de cifrado del host. Por ejemplo, supongamos que agrega una máquina virtual cifrada a un host independiente. El modo de cifrado de host no está establecido. Si se tienen los privilegios correspondientes en el host, el modo de cifrado cambiará automáticamente.

Supongamos que el clúster tiene tres hosts ESXi: A, B y C. Debe crear una máquina virtual cifrada en el host A. Lo que suceda dependerá de varios factores.

- Si ya se ha establecido el cifrado para los hosts A, B y C, solo se necesitan los privilegios **Operaciones criptográficas.Cifrar nuevo** para crear la máquina virtual.
- Si los hosts A y B se establecen para el cifrado de host y el C no lo está, el sistema procede de la siguiente manera.
  - Supongamos que tiene los privilegios **Operaciones criptográficas.Cifrar nuevo** y los privilegios **Operaciones criptográficas.Registrar host** en cada host. En este caso, el proceso de cifrado establece el modo de cifrado de host en el host C e inserta la clave en cada host del clúster.

    En este caso, también puede establecer explícitamente el modo de cifrado de host en el host C.
  - Suponga que solo tiene los privilegios **Operaciones criptográficas.Cifrar nuevo** en la máquina virtual o en una carpeta de máquinas virtuales. En ese caso, la creación de máquinas virtuales se completará correctamente y la clave estará disponible en el host A y el host B. El host C permanecerá desactivado para el cifrado y no tendrá la clave de la máquina virtual.
- Si ninguno de los hosts tiene configurado el modo de cifrado de host y usted cuenta con los privilegios **Operaciones criptográficas.Registrar host** en el host A, el proceso de creación de máquinas virtuales habilitará el cifrado de hosts en dicho host. De lo contrario, se producirá un error para los hosts B y C.

- También puede utilizar vSphere API para establecer el modo de cifrado de un clúster en "forzar la habilitación". Forzar habilitación hace que todos los hosts del clúster sean "seguros" desde el punto de vista de cifrado, es decir, que vCenter Server haya instalado una clave de host en el host. Consulte *Guía de programación de vSphere Web Services SDK*.

Requisitos de espacio de disco al cifrar máquinas virtuales

Al cifrar una máquina virtual existente, se necesita al menos el doble de espacio que el que utiliza actualmente la máquina virtual.

Qué es vSphere vMotion cifrado

vSphere vMotion cifrado garantiza la confidencialidad, la integridad y la autenticidad de los datos que se transfieren con vSphere vMotion. vSphere admite vMotion cifrado de máquinas virtuales sin cifrar y cifradas en varias instancias de vCenter Server.

vSphere vMotion siempre utiliza cifrado para migrar máquinas virtuales cifradas. Para las máquinas virtuales sin cifrar, se puede seleccionar una de las opciones de vSphere vMotion cifrado.

Qué se cifra en vSphere vMotion cifrado

En los discos cifrados, los datos se transmiten cifrados en todos los casos. En los discos sin cifrar, se aplica lo siguiente:

- Si los datos de disco se transfieren dentro de un host (es decir, sin cambiar el host, cambiando solo el almacén de datos), la transferencia no estará cifrada.
- Si los datos de disco se transfieren entre hosts y se utiliza vMotion cifrado, la transferencia estará cifrada. Si no se utiliza vMotion cifrado, la transferencia no estará cifrada.

En las máquinas virtuales cifradas, siempre se utiliza vSphere vMotion cifrado para la migración con vSphere vMotion. No se puede desactivar vSphere vMotion cifrado en las máquinas virtuales cifradas.

Estados de vSphere vMotion cifrados para máquinas virtuales sin cifrar

En las máquinas virtuales sin cifrar, se puede establecer vSphere vMotion cifrado en uno de los siguientes estados. El valor predeterminado es Oportunista.

Deshabilitado

No se utiliza vSphere vMotion cifrado.

Oportunista

Se utiliza vSphere vMotion cifrado si los hosts de origen y destino lo admiten. Solo los hosts ESXi de la versión 6.5 y posterior admiten vSphere vMotion cifrado.

Obligatorio

Solo se permite vSphere vMotion cifrado. Si el host de origen o de destino no admite vSphere vMotion cifrado, no se permite la migración con vSphere vMotion.

Cuando se cifra una máquina virtual, la máquina virtual conserva un registro de la configuración actual de vSphere vMotion cifrado. Si posteriormente se desactiva el cifrado para la máquina virtual, la configuración de vMotion cifrado sigue siendo Obligatorio hasta que se modifica de forma explícita la configuración. Es posible modificar la configuración mediante la opción **Editar configuración**.

Consulte la documentación de *Administrar vCenter Server y hosts* para obtener información sobre la forma de activar y desactivar vSphere vMotion cifrado en máquinas virtuales sin cifrar.

Nota Actualmente, hay que utilizar las API de vSphere para migrar o clonar máquinas virtuales cifradas entre instancias de vCenter Server. Consulte la *Guía de programación de vSphere Web Services SDK* y *Referencia de vSphere Web Services API*.

Migrar o clonar máquinas virtuales cifradas en varias instancias de vCenter Server

vSphere vMotion admite la migración y la clonación de máquinas virtuales cifradas en varias instancias de vCenter Server.

Al migrar o clonar máquinas virtuales cifradas en varias instancias de vCenter Server, deben configurarse las instancias de vCenter Server de origen y destino para compartir el proveedor de claves que se usó para cifrar la máquina virtual. Además, el nombre del proveedor de claves debe ser el mismo en las instancias de vCenter Server de origen y destino y tener las siguientes características.

- Proveedor de claves estándar: el mismo servidor de claves (o servidores de claves) debe estar en el proveedor de claves.
- Proveedor de claves de confianza: el mismo vSphere Trust Authority servicio debe estar configurado en el host de destino.
- vSphere Native Key Provider: debe tener el mismo KDK.

  Nota No se puede clonar ni migrar una máquina virtual cifrada mediante vSphere Native Key Provider a un host independiente, independientemente de que el host de origen resida en un clúster.

La instancia de vCenter Server de destino garantiza que el host ESXi de destino tenga configurado el modo de cifrado, lo que garantiza que el host esté "seguro" desde el punto de vista de cifrado.

Se requieren los siguientes privilegios al utilizar vSphere vMotion para migrar o clonar una máquina virtual cifrada en varias instancias de vCenter Server.

- Migrar: **Operaciones criptográficas.Migrar** en la máquina virtual
- Clonar: **Operaciones criptográficas.Clonar** en la máquina virtual

Asimismo, la instancia de vCenter Server de destino debe tener el privilegio **Operaciones criptográficas.Cifrar nuevo**. Si el host ESXi de destino no está en modo "seguro", el privilegio **Operaciones criptográficas.Registrar host** también debe estar en la instancia de vCenter Server de destino.

Algunas tareas no se permiten al migrar máquinas virtuales (sin cifrar o cifradas), ya sea en el mismo vCenter Server o en instancias de vCenter Server.

- No se puede cambiar la directiva de almacenamiento de máquina virtual.
- No se puede realizar un cambio de clave.

Nota Puede cambiar la directiva de almacenamiento de máquina virtual al clonar máquinas virtuales.

Requisitos mínimos para migrar o clonar máquinas virtuales cifradas en varias instancias de vCenter Server

Los requisitos mínimos de versión para la migración o la clonación de máquinas virtuales cifradas de proveedores de claves estándar en instancias de vCenter Server mediante vSphere vMotion son los siguientes:

- Las instancias de vCenter Server de origen y destino deben ser de la versión 7.0 o posterior.
- Los hosts de ESXi de origen y destino deben ser de la versión 6.7 o posterior.

Los requisitos mínimos de versión para la migración o la clonación de máquinas virtuales cifradas de proveedores de claves de confianza en instancias de vCenter Server mediante vSphere vMotion son los siguientes:

- Debe configurarse el servicio de vSphere Trust Authority para el host de destino y se debe atestar el host de destino.
- El cifrado no puede cambiar en la migración. Por ejemplo, un disco sin cifrar no se puede cifrar mientras la máquina virtual está migrando a un almacenamiento nuevo.
- Puede migrar una máquina virtual cifrada estándar a un host de confianza. El nombre del proveedor de claves debe ser el mismo en las instancias de vCenter Server de origen y destino.
- No se puede migrar una máquina virtual cifrada de vSphere Trust Authority a un host que no es de confianza.

Proveedor de claves de confianza vMotion y Cross-vCenter Server vMotion

El proveedor de claves de confianza es totalmente compatible con vMotion ESXi hosts.

Se admite vMotion entre instancias de vCenter Server, pero con las siguientes restricciones.

1. Se debe configurar el servicio de confianza requerido en el host de destino y se debe atestar el host de destino.
2. El cifrado no puede cambiar en la migración. Por ejemplo, un disco no se puede cifrar mientras la máquina virtual se migra al almacenamiento nuevo.

Al realizar operaciones de vMotion entre instancias de vCenter Server, vCenter Server comprueba que el proveedor de claves de confianza está disponible en el host de destino y que el host tiene acceso a él.

vSphere Native Key Provider vMotion y Cross-vCenter Server vMotion

vSphere Native Key Provider es compatible con vMotion y vMotion cifrado en ESXi hosts. Cross-vCenter Server vMotion es compatible si vSphere Native Key Provider está configurado en el host de destino.

Prácticas recomendadas de cifrado de máquinas virtuales

Siga las prácticas recomendadas de cifrado de máquinas virtuales para evitar problemas futuros, por ejemplo, al generar un paquete de `vm-support`.

Prácticas recomendadas para comenzar con el cifrado de máquinas virtuales

Para evitar problemas a la hora de utilizar el cifrado de máquinas virtuales, siga estas prácticas recomendadas generales.

- No cifre ninguna máquina virtual de vCenter Server Appliance.
- Si se produce un error en el host ESXi, recupere el paquete de soporte lo antes posible.
  La clave de host debe estar disponible para generar un paquete de soporte que utilice una contraseña o para descifrar un volcado de núcleo. Si el host se reinicia, es posible que se cambie la clave de host. En caso de que esto suceda, ya no se podrá generar un paquete de soporte con una contraseña ni descifrar volcados de núcleo en el paquete de soporte con la clave de host.
- Administre los nombres de proveedor de claves con cuidado. Si cambia el nombre de proveedor de claves por un servidor de claves que ya está en uso, la máquina virtual cifrada con las claves de ese servidor de claves pasa a tener el estado bloqueado durante el encendido o el registro. En ese caso, elimine el servidor de claves de vCenter Server y agréguelo con el nombre de proveedor de claves que utilizó al comienzo.

- No edite los archivos VMX ni los archivos de descriptores de VMDK. Estos archivos contienen el paquete de cifrado. Es posible que la máquina virtual no se pueda recuperar debido a los cambios realizados y que el problema de recuperación no se pueda solucionar.
- El proceso de cifrado de máquinas virtuales de vSphere cifra los datos en el host antes de escribir los datos en el almacenamiento. La eficacia de las funciones de almacenamiento back-end (como la desduplicación, la compresión, la replicación, etc.) puede verse afectada cuando las máquinas virtuales se cifran de esta manera.
- Si utiliza varias capas de cifrado, por ejemplo, cifrado de máquinas virtuales de vSphere y cifrado en el invitado (BitLocker, dm-crypt, etc.), el rendimiento general de la máquina virtual puede verse afectado, ya que los procesos de cifrado usan recursos adicionales de CPU y memoria.
- Asegúrese de que las copias replicadas de las máquinas virtuales cifradas con el cifrado de máquinas virtuales de vSphere tengan acceso a las claves de cifrado en el sitio de recuperación. Para los proveedores de claves estándar, esto se controla como parte del diseño del sistema de administración de claves, fuera de vSphere. Para vSphere Native Key Provider, asegúrese de que exista una copia de seguridad de la instancia de vSphere Native Key Provider y esté protegida contra la pérdidas. Para obtener más información, consulte Hacer una copia de seguridad de vSphere Native Key Provider.
- El cifrado requiere gran consumo de CPU. AES-NI mejora significativamente el rendimiento del cifrado. Habilite AES-NI en el BIOS.

Prácticas recomendadas para volcados de núcleo cifrados

Siga estas prácticas recomendadas para evitar problemas cuando desee examinar un volcado de núcleo a fin de diagnosticar un problema.

- Establezca una directiva con respecto a los volcados de núcleo. Los volcados de núcleo están cifrados porque pueden contener información confidencial, por ejemplo, claves. Si descifra un volcado de núcleo, asuma que contiene información confidencial. Los volcados de núcleo de ESXi pueden contener claves para el host ESXi y para las máquinas virtuales que este contiene. Después de descifrar un volcado de núcleo, considere cambiar la clave del host y volver a cifrar las máquinas virtuales cifradas. Puede realizar ambas tareas con vSphere API.

  Consulte Cifrado de máquinas virtuales de vSphere y volcados de núcleo para obtener detalles.
- Siempre utilice una contraseña cuando recopile un paquete de `vm-support`. Puede especificar la contraseña cuando genera el paquete de soporte de vSphere Client o puede utilizar el comando `vm-support`.

La contraseña vuelve a cifrar los volcados de núcleo que utilizan claves internas de manera que estos volcados empleen claves basadas en la contraseña. Posteriormente, se puede usar la contraseña para descifrar cualquier volcado de núcleo cifrado que pudiera estar incluido en el paquete de soporte. El uso de la opción de contraseña no afecta a los volcados de núcleo sin cifrar ni los registros.

- La contraseña que especificó durante la creación del paquete de `vm-support` no persiste en los componentes de vSphere. Es su responsabilidad llevar un registro de las contraseñas de los paquetes de soporte.
- Antes de cambiar la clave de host, genere un paquete de `vm-support` con una contraseña. Más adelante, puede usar la contraseña para acceder a todos los volcados de núcleo que se hayan cifrado con la clave de host anterior.

Prácticas recomendadas para la administración del ciclo de vida de claves

Implemente prácticas recomendadas que garanticen la disponibilidad del servidor de claves y supervise las claves en el servidor de claves.

- Usted es responsable de contar con las directivas que garanticen la disponibilidad del servidor de claves.

  Si el servidor de claves no está disponible, no se pueden realizar operaciones de máquinas virtuales que requieren que vCenter Server solicite la clave del servidor de claves. Eso significa que las máquinas virtuales en ejecución siguen ejecutándose, y puede encenderlas, apagarlas y volver a configurarlas. No obstante, no puede reubicar la máquina virtual en un host que no tiene la información de la clave.

  La mayoría de las soluciones de servidor de claves incluyen funciones de alta disponibilidad. Puede utilizar vSphere Client o la API para especificar un proveedor de claves y los servidores de proveedor de claves asociados.

  Nota A partir de la versión 7.0 Update 2, las máquinas virtuales cifradas y los TPM virtuales pueden seguir funcionando incluso cuando el servidor de claves está desconectado temporalmente o no está disponible. Los hosts ESXi pueden conservar las claves de cifrado para continuar con el cifrado y las operaciones de vTPM. Consulte Persistencia de claves de vSphere en hosts ESXi.

- Es su responsabilidad llevar un registro de las claves y encontrar soluciones si las claves de las máquinas virtuales actuales no tienen el estado Activa.

  El estándar KMIP define los siguientes estados para las claves:

  - Preactiva
  - activa
  - Desactivada
  - Comprometida

- Destruida
- Comprometida destruida

El cifrado de máquinas virtuales de vSphere utiliza solo claves con el estado Activa para cifrar. Si la clave está en el estado Preactiva, el cifrado de máquinas virtuales de vSphere la activa. Si el estado de la clave es Desactivada, Comprometida, Destruida o Comprometida destruida, no se pueden cifrar una máquina ni un disco virtuales con esa clave.

Las máquinas virtuales que usan estas claves seguirán funcionando cuando las claves tengan otros estados. La correcta ejecución de una operación de clonación o migración dependerá de si la clave ya existe en el host.

- Si la clave existe en el host de destino, la operación se realiza correctamente incluso si la clave no tiene el estado Activa en el servidor de claves.
- Si las claves de máquina virtual y disco virtual no están en el host de destino, vCenter Server debe recuperar las claves del servidor de claves. Si el estado de la clave es Desactivada, Comprometida, Destruida o Comprometida destruida, vCenter Server muestra un error y la operación no se realiza correctamente.

Una operación de clonación o de migración se realiza correctamente si la clave ya está en el host. Se produce un error en la operación si vCenter Server debe extraer las claves del servidor de claves.

Si una clave no tiene el estado Activa, vuelva a introducir la clave con la API. Consulte la *Guía de programación de vSphere Web Services SDK*.

- Desarrolle directivas de rotación de claves para que las claves se retiren y se transfieran después de un momento específico.
  - Proveedor de claves de confianza: cambie la clave principal de un proveedor de claves de confianza.
  - vSphere Native Key Provider: cambie el `key_id` de una instancia de vSphere Native Key Provider.

Prácticas recomendadas para la copia de seguridad y la restauración

Establezca directivas para las operaciones de copias de seguridad y restauración.

- No todas las arquitecturas de copias de seguridad son compatibles. Consulte Interoperabilidad del cifrado de máquinas virtuales.
- Establezca directivas para las operaciones de restauración. Debido a que las copias de seguridad siempre incluyen texto no cifrado, cifre las máquinas virtuales inmediatamente después de que finalice la restauración. Puede especificar que se cifre la máquina virtual como parte de la operación de restauración. Si fuera posible, cifre la máquina virtual como parte del proceso de restauración para evitar que se divulgue información confidencial. Para cambiar la directiva de cifrado de cualquier disco que esté relacionado con la máquina virtual, cambie la directiva de almacenamiento de ese disco.

- Debido a que los archivos de inicio de la máquina virtual están cifrados, asegúrese de que las claves de cifrado estén disponibles en el momento de una restauración.

Prácticas recomendadas para el rendimiento del cifrado

- El rendimiento del cifrado depende de la velocidad de la CPU y del almacenamiento.
- El cifrado de las máquinas virtuales existentes lleva más tiempo que el cifrado de una máquina virtual durante la creación. En lo posible, cifre la máquina virtual al crearla.

Prácticas recomendadas para la directiva de almacenamiento de muestra

No modifique la directiva de almacenamiento de muestra de cifrado de una máquina virtual en paquete. En lugar de ello, clone la directiva y edite el clon.

Nota No existe ninguna manera automatizada de restaurar la directiva de cifrado de una máquina virtual a la configuración original.

Consulte la documentación de *Almacenamiento de vSphere* si desea obtener información para personalizar las directivas de almacenamiento.

Prácticas recomendadas para eliminar claves de cifrado

Para asegurarse de que las claves de cifrado se eliminen de un clúster, después de quitar, eliminar del registro o mover la máquina virtual cifrada a otra instancia de vCenter Server, reinicie los hosts ESXi en el clúster.

Advertencias de cifrado de máquinas virtuales

Revise las advertencias de cifrado de máquinas virtuales para evitar problemas futuros.

Si desea comprender qué dispositivos y funciones no se pueden usar con el cifrado de máquinas virtuales, consulte Interoperabilidad del cifrado de máquinas virtuales.

Limitaciones de máquinas virtuales cifradas

Tenga en cuenta las siguientes advertencias cuando planifique una estrategia de cifrado de máquinas virtuales.

- Cuando clona una máquina virtual cifrada o realiza una operación de Storage vMotion, puede intentar cambiar el formato del disco. Esas conversiones no siempre se realizan correctamente. Por ejemplo, si clona una máquina virtual e intenta cambiar el disco de un formato grueso sin puesta a cero diferido a un formato fino, el disco de la máquina virtual conserva el formato grueso sin puesta a cero diferido.

- Si separa un disco de una máquina virtual, no se conservará la información de la directiva de almacenamiento del disco virtual.
  - Si el disco virtual está cifrado, debe establecer explícitamente la directiva de almacenamiento en la directiva de cifrado de la máquina virtual o en una directiva de almacenamiento que incluya el cifrado.
  - Si el disco virtual no está cifrado, puede cambiar la directiva de almacenamiento cuando agrega el disco a la máquina virtual.

  Consulte Cifrado de disco virtual para obtener detalles.
- Descifre los volcados de núcleo antes de mover una máquina virtual a un clúster diferente.

  vCenter Server no almacena las claves del servidor de claves, solo realiza el seguimiento de los identificadores de claves. Por este motivo, vCenter Server no almacena claves de hosts ESXi de forma persistente. Sin embargo, en vSphere 7.0 Update 2 y versiones posteriores, los dispositivos cifrados pueden funcionar incluso cuando se interrumpe el acceso a un servidor de claves. Consulte Persistencia de claves de vSphere en hosts ESXi.

  En determinadas circunstancias, por ejemplo, si mueve el host ESXi a un clúster distinto y reinicia el host, vCenter Server asigna una clave nueva al host. No se puede descifrar ningún volcado de núcleo actual con la clave de host nueva.
- Una máquina virtual cifrada no admite la exportación de OVF.
- No se admite el uso de VMware Host Client para registrar una máquina virtual cifrada.

Estado bloqueado de una máquina virtual

Si falta la clave de la máquina virtual, o una o más claves del disco virtual, la máquina virtual entra en un estado bloqueado. En un estado bloqueado, no se pueden realizar operaciones de máquinas virtuales.

- Si cifra una máquina virtual y sus discos desde vSphere Client, se utiliza la misma clave en ambos casos.
- Si realiza el cifrado con la API, puede usar distintas claves de cifrado para la máquina virtual y los discos. En un caso así, si intenta encender una máquina virtual y falta una de las claves de disco, no podrá concretar la operación de encendido. Si retira el disco virtual, podrá encender la máquina virtual.

Consulte Resolver problemas de claves de cifrado que faltan si desea obtener sugerencias de solución de problemas.

Interoperabilidad del cifrado de máquinas virtuales

El cifrado de máquinas virtuales de vSphere tiene algunas limitaciones con respecto a los dispositivos y las funciones con los que puede interoperar.

Las siguientes limitaciones y comentarios hacen referencia al uso del cifrado de máquinas virtuales de vSphere. Para obtener información similar sobre cómo usar el cifrado de vSAN, consulte la documentación de *Administrar VMware vSAN*.

Limitaciones de ciertas tareas de cifrado

Se aplican algunas restricciones al realizar ciertas tareas en una máquina virtual cifrada.

- Para la mayoría de las operaciones cifradas de máquinas virtuales, debe apagar la máquina virtual. Se puede clonar una máquina virtual cifrada y se puede realizar un cifrado superficial mientras la máquina virtual está encendida.

  Nota Las máquinas virtuales configuradas con controladoras IDE deben apagarse para realizar una operación de regeneración de claves superficial.

- No se puede realizar una repetición de cifrado profundo en una máquina virtual con instantáneas. Puede realizar una repetición de cifrado superficial en una máquina virtual con instantáneas.

Dispositivos del módulo de plataforma de confianza virtual y cifrado de máquinas virtuales de vSphere

Un módulo de plataforma de confianza virtual (virtual Trusted Platform Module, vTPM) es una representación basada en software de un chip de módulo de plataforma de confianza 2.0 físico. Se puede agregar un vTPM a una máquina virtual nueva o existente. Para agregar un vTPM a una máquina virtual, debe configurar un proveedor de claves en el entorno de vSphere. Cuando se configura un vTPM, se cifran los archivos de "inicio" de la máquina virtual (intercambio de memoria, archivos de NVRAM, etc.). Los archivos de disco, o archivos VMDK, no se cifran automáticamente. Puede optar por agregar el cifrado de forma explícita para los discos de la máquina virtual.

Precaución Al clonar una máquina virtual, se duplica toda la máquina virtual, incluidos los dispositivos virtuales, como un vTPM. También se duplica la información almacenada en el vTPM, incluidas las propiedades del vTPM que el software puede utilizar para determinar la identidad de un sistema.

En vSphere 8.0 y versiones posteriores, al clonar una máquina virtual que incluye un vTPM, puede optar por comenzar con un nuevo vTPM vacío, que obtiene sus propios secretos e identidades.

Cifrado y estado suspendido de máquinas virtuales de vSphere e instantáneas

Puede reanudar la operación desde una máquina virtual cifrada en estado de suspensión o revertir a una instantánea de memoria de una máquina cifrada. Puede migrar una máquina virtual cifrada con una instantánea de memoria y el estado de suspensión entre hosts ESXi.

Cifrado de máquinas virtuales de vSphere e IPv6

Puede utilizar el cifrado de máquinas virtuales de vSphere con el modo IPv6 puro o en modo mixto. Puede configurar el servidor de claves con direcciones IPv6. Puede configurar tanto vCenter Server como el servidor de claves solo con direcciones IPv6.

Limitaciones sobre la clonación en el cifrado de máquinas virtuales de vSphere

Para todos los tipos de proveedores de claves, la clonación se admite de forma condicional. Puede cambiar las claves de cifrado al clonar. Algunas funciones de clonación no son compatibles con el cifrado de máquinas virtuales de vSphere.

- Se admite la clonación completa. El clon hereda el estado de cifrado del elemento principal, incluidas las claves. Puede cifrar el clon completo o volver a cifrarlo para usar claves nuevas, o descifrar el clon completo.

  Se admiten los clones vinculados y el clon hereda el estado de cifrado del elemento principal, incluidas las claves. No se puede descifrar el clon vinculado ni volver a cifrarlo con claves distintas.

  Nota Compruebe que otras aplicaciones admitan clones vinculados. Por ejemplo, VMware Horizon® 7 admite clones completos e instantáneos, pero no clones vinculados.

- La opción de clon instantáneo es compatible con todos los tipos de proveedores de claves, pero no se pueden cambiar las claves de cifrado en el clon.
- Puede crear una máquina virtual de clon vinculado a partir de una máquina virtual cifrada. La máquina virtual de clon vinculado contiene las mismas claves. Puede regenerar claves en los archivos "de inicio" de máquina virtual cifrados de un clon vinculado, pero no puede regenerar claves para los discos.

Limitaciones con vSphere Native Key Provider

Algunas operaciones no son compatibles con vSphere Native Key Provider.

- No puede usar vSphere Native Key Provider para cifrar máquinas virtuales en un host independiente. El host debe residir en un clúster para usar vSphere Native Key Provider.
- No se puede mover un host que contenga máquinas virtuales cifradas mediante vSphere Native Key Provider a un clúster diferente a menos que el clúster de destino contenga el mismo vSphere Native Key Provider. (Las máquinas virtuales cifradas en el host movido se bloquean cuando las claves de cifrado no están presentes y el clúster de destino no tiene el mismo vSphere Native Key Provider).
- No se puede registrar una máquina virtual cifrada por vSphere Native Key Provider en un host heredado debido a la falta de compatibilidad con vSphere Native Key Provider.
- No se puede registrar una máquina virtual cifrada por vSphere Native Key Provider en un host independiente debido a los requisitos para que el host resida en un clúster.

Configuraciones de disco no compatibles con el cifrado de máquina virtual de vSphere

No se admiten ciertos tipos de configuraciones de disco de máquina virtual con el cifrado de máquinas virtuales de vSphere.

- Asignación de dispositivos sin formato (Raw Device Mapping, RDM). Sin embargo, se admiten vSphere Virtual Volumes (vVols).
- Multiescritura o discos compartidos (MSCS, WSFC u Oracle RAC). Los archivos de "inicio" de máquina virtual cifrados son compatibles con los discos de multiescritura. Los discos virtuales cifrados no son compatibles con los discos de multiescritura. Si intenta seleccionar Multiescritura en la página **Editar configuración** de la máquina virtual con discos virtuales cifrados, se desactivará el botón **Aceptar**.

Varias limitaciones en el cifrado de máquinas virtuales de vSphere

Entre las funciones que no funcionan con el cifrado de máquinas virtuales de vSphere se encuentran las siguientes.

- vSphere ESXi Dump Collector
- Biblioteca de contenido
  - Las bibliotecas de contenido admiten dos tipos de plantillas, el tipo de plantilla de OVF y el tipo de plantilla de máquina virtual. No puede exportar una máquina virtual cifrada al tipo de plantilla de OVF. OVF Tool no admite máquinas virtuales cifradas. Puede crear plantillas de máquina virtual cifradas mediante el tipo de plantilla de máquina virtual. En vSphere 8.0 y versiones posteriores, el comando `ovftool` incluye una opción para agregar un marcador de posición de vTPM al archivo de descriptor OVF. Al implementar una máquina virtual desde una plantilla de este tipo, vCenter Server crea un vTPM con secretos únicos en la máquina virtual de destino. Consulte el documento *Administrar máquinas virtuales de vSphere*.
- El software para realizar copias de seguridad de discos virtuales cifrados debe utilizar VMware vSphere Storage API - Data Protection (VADP) para realizar copias de seguridad de los discos en el modo agregado en caliente o en el modo NBD con SSL habilitado. Sin embargo, no se admiten todas las soluciones de copia de seguridad que utilizan VADP para la copia de seguridad del disco virtual. Consulte con su proveedor de copias de seguridad para obtener más información.
  - Las soluciones de modo de transporte SAN de VADP no son compatibles con la copia de seguridad de discos virtuales cifrados.
  - Las soluciones de agregado en caliente de VADP son compatibles con los discos virtuales cifrados. El software de copia de seguridad debe admitir el cifrado de la máquina virtual proxy que se utiliza como parte del flujo de trabajo de copia de seguridad de agregado en caliente. El proveedor debe poseer el privilegio **Operaciones criptográficas.Cifrar máquina virtual**.

- Las soluciones de copia de seguridad que utilizan los modos de transporte NBD-SSL son compatibles para realizar copias de seguridad de discos virtuales cifrados. La aplicación del proveedor debe poseer el privilegio **Operaciones criptográficas.Acceso directo**.
- No se pueden enviar los resultados de una máquina virtual cifrada a un puerto serie ni a un puerto paralelo. Aunque parezca que la configuración se realiza correctamente, los resultados se envían a un archivo.
- El cifrado de máquinas virtuales de vSphere no es compatible con VMware Cloud on AWS. Consulte la documentación *Administrar el centro de datos de VMware Cloud on AWS*.

Persistencia de claves de vSphere en hosts ESXi

En vSphere 7.0 Update 2 y versiones posteriores, las máquinas virtuales cifradas y los TPM virtuales pueden seguir funcionando opcionalmente incluso cuando el servidor de claves está desconectado temporalmente o no está disponible. Los hosts ESXi pueden conservar las claves de cifrado para continuar con el cifrado y las operaciones de vTPM.

Antes de vSphere 7.0 Update 2, las máquinas virtuales cifradas y los vTPM requieren que el servidor de claves esté siempre disponible para funcionar. En vSphere 7.0 Update 2 y versiones posteriores, los dispositivos cifrados pueden funcionar incluso cuando se interrumpe el acceso a un servidor de claves.

En vSphere 7.0 Update 3 y versiones posteriores, los clústeres de vSAN cifrados también pueden funcionar incluso cuando se interrumpe el acceso a un proveedor de claves.

Nota La persistencia de claves no es necesaria cuando se utiliza vSphere Native Key Provider. vSphere Native Key Provider está diseñado de fábrica para ejecutarse sin necesidad de acceder a un servidor de claves. Consulte la siguiente sección "Persistencia de claves y vSphere Native Key Provider".

Cómo funciona la persistencia de claves en hosts ESXi

Cuando se utiliza un proveedor de claves estándar, el host de ESXi se basa en vCenter Server para administrar las claves de cifrado. Cuando se utiliza un proveedor de claves de confianza, el host de ESXi se basa directamente en los hosts de Trust Authority para las claves, y vCenter Server no está involucrado. vSphere Native Key Provider controla las claves de forma diferente. Consulte la siguiente sección para obtener más información.

Independientemente del tipo de proveedor de claves, el host ESXi obtiene las claves inicialmente y las conserva en su memoria caché de claves. Si el host ESXi se reinicia, pierde su memoria caché de claves. El host ESXi vuelve a solicitar las claves, ya sea del servidor de claves (proveedor de claves estándar) o de los hosts de Trust Authority (proveedor de claves de confianza). Cuando el host ESXi intenta obtener claves y el servidor de claves está sin conexión o no se puede acceder a él, los vTPM y el cifrado de cargas de trabajo no pueden funcionar. Para las implementaciones de tipo Edge, en las que normalmente no se implementa un servidor de claves en el sitio, la pérdida de conectividad con un servidor de claves puede provocar un tiempo de inactividad innecesario para las cargas de trabajo cifradas.

En vSphere 7.0 Update 2 y versiones posteriores, las cargas de trabajo cifradas pueden seguir funcionando incluso cuando el servidor de claves está sin conexión o no se puede acceder a él. Si el host ESXi tiene un TPM, las claves de cifrado se conservan en el TPM después de reiniciar. Por lo tanto, incluso si un host ESXi se reinicia, no es necesario que solicite claves de cifrado. Además, las operaciones de cifrado y descifrado pueden continuar cuando el servidor de claves no está disponible, ya que las claves han persistido en el TPM. Básicamente, en función del proveedor de claves, cuando el servidor de claves o los hosts de Trust Authority no están disponibles, puede seguir ejecutando cargas de trabajo cifradas "sin servidor de claves". Además, los vTPM también pueden seguir funcionando aunque no se pueda acceder al servidor de claves.

Persistencia de claves y vSphere Native Key Provider

Cuando se utiliza un vSphere Native Key Provider, vSphere genera las claves y no se requiere ningún servidor de claves. Los hosts ESXi obtienen una clave de derivación de claves (Key Derivation Key, KDK), que se utiliza para derivar otras claves. Después de recibir el KDK y generar otras claves, los hosts ESXi no necesitan acceso a vCenter Server para realizar operaciones de cifrado. Básicamente, vSphere Native Key Provider siempre se ejecuta "sin servidor de claves".

El KDK persiste en un host ESXi de forma predeterminada incluso después del reinicio, e incluso cuando vCenter Server no está disponible después de que se reinicie el host.

Puede activar la persistencia de claves con vSphere Native Key Provider, pero normalmente no es necesario. Los hosts ESXi tienen acceso completo a vSphere Native Key Provider, por lo que la persistencia adicional de las claves es redundante. Un caso práctico para activar la persistencia de claves con vSphere Native Key Provider es cuando también se configuró un proveedor de claves estándar (servidor KMIP externo).

Cómo configurar la persistencia de claves

Para activar o desactivar la persistencia de claves, consulte Activar y desactivar la persistencia de claves en un host ESXi.

Configurar y administrar un proveedor de claves estándar

7

El uso de un proveedor de claves estándar en el entorno vSphere requiere algo de preparación. Una vez que el entorno está configurado, se pueden crear máquinas virtuales y discos virtuales cifrados, así como cifrar discos y máquinas virtuales existentes.

Una vez que el entorno está configurado para un proveedor de claves estándar, se puede usar vSphere Client para crear máquinas virtuales y discos virtuales cifrados, así como cifrar discos y máquinas virtuales existentes. Consulte Capítulo 10 Usar el cifrado en el entorno de vSphere.

Se pueden usar la API y la crypto-util CLI para realizar tareas adicionales. Consulte la *Guía de programación de vSphere Web Services SDK* para ver la documentación de API y la ayuda de la línea de comandos `crypto-util` para ver detalles de esa herramienta.

Lea los siguientes temas a continuación:

Qué es un proveedor de claves estándar

Puede utilizar un proveedor de claves estándar para realizar tareas de cifrado de máquinas virtuales.

En vSphere, un proveedor de claves estándar obtiene claves de cifrado directamente de un servidor de claves, y vCenter Server distribuye las claves a los hosts ESXi necesarios en un centro de datos.

Puede agregar proveedores de claves estándar aparte para distintos usuarios y establecer el proveedor de claves estándar predeterminado.

Requisitos del proveedor de claves estándar

- vSphere 6.5 o posterior
- Un servidor de claves externo (KMS)

El servidor de claves debe admitir el estándar del protocolo de interoperabilidad para la administración de claves (KMIP) 1.1. Consulte la *Matrices de compatibilidad de vSphere* para obtener detalles.

Puede encontrar información sobre los proveedores del servidor de claves certificado de VMware en la Guía de compatibilidad de VMware, en la sección Plataforma y cómputo. Si selecciona las guías de compatibilidad, puede abrir la documentación de compatibilidad del servidor de administración de claves (KMS). Esta documentación se actualiza con frecuencia.

Privilegios del proveedor de claves estándar

Los proveedores de claves estándar utilizan los privilegios **Cryptographer.***. Consulte Privilegios de operaciones de cifrado.

Configurar el proveedor de claves estándar

Antes de comenzar con las tareas de cifrado de máquinas virtuales, debe configurar el proveedor de claves estándar.

La configuración de un proveedor de claves estándar incluye agregar el proveedor de claves y establecer confianza con el servidor de claves. Cuando agrega un proveedor de claves, se le solicita que lo establezca como predeterminado. Puede cambiar explícitamente el proveedor de claves predeterminado. vCenter Server aprovisiona claves del proveedor de claves predeterminado.

Nota Lo que anteriormente se denominaba clúster del servidor de administración de claves en vSphere 6.5 y 6.7 ahora se conoce como proveedor de claves.

Agregar un proveedor de claves estándar mediante vSphere Client

Puede agregar un proveedor de claves estándar al sistema de vCenter Server desde vSphere Client o con la API pública.

vSphere Client permite agregar un proveedor de claves estándar al sistema de vCenter Server y establecer la confianza entre el servidor de claves y vCenter Server.

- Puede agregar varios servidores de claves del mismo proveedor.
- Si el entorno admite soluciones de diferentes proveedores, es posible agregar varios proveedores de claves.
- Si el entorno incluye varios proveedores de claves y se elimina el proveedor predeterminado, se debe establecer explícitamente otro proveedor predeterminado.
- Puede configurar el servidor de claves con direcciones IPv6.
  - Tanto el sistema de vCenter Server como el servidor de claves pueden configurarse únicamente con direcciones IPv6.

Requisitos previos

- Compruebe que el servidor de claves (KMS) se encuentre en la *guía de compatibilidad de VMware para los servidores de administración de claves (Key Management Servers, KMS)*, que cumpla con KMIP 1.1, y que pueda ser un servidor y una fundición de claves simétricas.
- Compruebe que cuenta con los privilegios necesarios: **Operaciones criptográficas.Administrar servidores de claves**.
- Asegúrese de que el servidor de claves está altamente disponible. La pérdida de conexión con el servidor de claves, como la que ocurre durante una interrupción de energía o un evento de recuperación ante desastres, hace que no se pueda acceder a las máquinas virtuales cifradas.

  Nota En vSphere 7.0 Update 2 y versiones posteriores, las máquinas virtuales cifradas y los TPM virtuales pueden seguir funcionando incluso cuando el servidor de claves está desconectado temporalmente o no está disponible. Consulte Persistencia de claves de vSphere en hosts ESXi.

- Considere detenidamente las dependencias de su infraestructura en el servidor de claves. Algunas soluciones de KMS se proporcionan como dispositivos virtuales, lo que permite crear un bucle de dependencia u otro problema de disponibilidad con una ubicación deficiente del dispositivo KMS.

Procedimiento

1 Inicie sesión en el sistema vCenter Server mediante vSphere Client.

2 Examine la lista de inventario y seleccione la instancia de vCenter Server.

3 Haga clic en **Configurar** y, en **Seguridad**, haga clic en **Proveedores de claves**.

4 Haga clic en **Agregar un proveedor de claves estándar** e introduzca la información del proveedor de claves.

Opción	Valor
Nombre	Nombre del proveedor de claves. Cada proveedor de claves lógico, independientemente de su tipo (proveedor de claves estándar, de confianza y nativo), debe tener un nombre único en todos los sistemas vCenter Server. Para obtener más información, consulte Nomenclatura de proveedor de claves.
KMS	Alias del servidor de claves (KMS).
Dirección	Dirección IP o FQDN del servidor de claves.
Puerto	Puerto en el cual vCenter Server se conecta al servidor de claves.
Servidor proxy	Dirección de servidor proxy opcional para conectarse al servidor de claves.
Puerto de proxy	Puerto de proxy opcional para conectarse al servidor de claves.

Opción	Valor
Nombre de usuario	Algunos proveedores de servidores de claves permiten a los usuarios especificar un nombre de usuario y una contraseña para aislar las claves de cifrado utilizadas por distintos usuarios o grupos. Especifique un nombre de usuario solo si el servidor de claves admite esta funcionalidad y si pretende utilizarla.
Contraseña	Algunos proveedores de servidores de claves permiten a los usuarios especificar un nombre de usuario y una contraseña para aislar las claves de cifrado utilizadas por distintos usuarios o grupos. Especifique una contraseña solo si el servidor de claves admite esta funcionalidad y si pretende utilizarla.

Puede hacer clic en **Agregar KMS** para agregar más servidores de claves.

5 Haga clic en **Agregar proveedor de claves**.

6 Haga clic en **Confianza**.

vCenter Server agrega el proveedor de claves y muestra el estado como Conectado.

Pasos siguientes

Consulte Establecer una conexión de confianza de proveedor de claves estándar mediante el intercambio de certificados.

Establecer una conexión de confianza de proveedor de claves estándar mediante el intercambio de certificados

Después de agregar el proveedor de claves estándar al sistema vCenter Server, puede establecer una conexión de confianza. El proceso exacto depende de los certificados que el proveedor de claves acepte y de la directiva de su empresa.

Requisitos previos

Agregue el proveedor de claves estándar.

Procedimiento

1 Desplácese hasta vCenter Server.

2 Haga clic en **Configurar** y seleccione **Proveedores de claves** en **Seguridad**.

3 Seleccione el proveedor de claves.

Se muestra el KMS para el proveedor de claves.

4 Seleccione el KMS.

5 En el menú desplegable **Establecer confianza**, seleccione **Hacer que KMS confíe en vCenter**.

6 Seleccione la opción adecuada para el servidor y complete los pasos.

Opción	Consulte
Certificado de CA raíz de vCenter Server	Usar la opción Certificado de CA raíz para establecer una conexión de confianza con el proveedor de claves estándar.
Certificado de vCenter Server	Usar la opción Certificado para establecer una conexión de confianza con el proveedor de claves estándar.
Cargar certificado y clave privada	Usar la opción Cargar certificado y clave privada para establecer una conexión de confianza con el proveedor de claves estándar.
Nueva solicitud de firma de certificado	Usar la opción Nueva solicitud de firma de certificado para establecer una conexión de confianza con el proveedor de claves estándar.

Usar la opción Certificado de CA raíz para establecer una conexión de confianza con el proveedor de claves estándar

Algunos proveedores de KMS requieren que se cargue el certificado de CA raíz al KMS. Este KMS establece una conexión de confianza con todos los certificados firmados por la entidad de certificación de raíz.

El certificado de CA raíz que utiliza el cifrado de máquinas virtuales de vSphere es un certificado autofirmado que se almacena en un almacén separado en VMware Endpoint Certificate Store (VECS) en el sistema de vCenter Server.

Nota Genere un certificado de CA raíz solo si desea reemplazar los certificados existentes. En ese caso, los demás certificados que están firmados por esa entidad de certificación raíz dejan de ser válidos. Se puede generar un nuevo certificado de CA raíz como parte de este flujo de trabajo.

Procedimiento

1 Desplácese hasta vCenter Server.

2 Haga clic en **Configurar** y seleccione **Proveedores de claves** en **Seguridad**.

3 Seleccione el proveedor de claves con el cual desea establecer una conexión de confianza.

Se muestra el servidor de claves (KMS) para el proveedor de claves.

4 En el menú desplegable **Establecer confianza**, seleccione **Hacer que KMS confíe en vCenter**.

5 Seleccione **Certificado de CA raíz de vCenter** y haga clic en **Siguiente**.

El cuadro de diálogo Descargar certificado de CA raíz se rellena con el certificado raíz que vCenter Server utiliza para el cifrado. Este certificado se almacena en el almacén VECS.

6 Copie el certificado en el portapapeles o descárguelo como un archivo.

7 Siga las instrucciones de su proveedor de KMS para cargar el certificado al sistema.

Nota Algunos proveedores de KMS requieren que el proveedor de KMS reinicie el KMS para seleccionar el certificado raíz que se cargó.

Pasos siguientes

Finalice el intercambio de certificados. Consulte Finalizar la configuración de confianza de un proveedor de claves estándar.

Usar la opción Certificado para establecer una conexión de confianza con el proveedor de claves estándar

Algunos proveedores de KMS requieren que se cargue el certificado de vCenter Server al KMS. Después de la carga, el KMS acepta el tráfico proveniente de un sistema con ese certificado.

vCenter Server genera un certificado para proteger las conexiones con el KMS. El certificado se almacena en un almacén de claves separado en VMware Endpoint Certificate Store (VECS) en el sistema de vCenter Server.

Procedimiento

1 Desplácese hasta vCenter Server.

2 Haga clic en **Configurar** y seleccione **Proveedores de claves** en **Seguridad**.

3 Seleccione el proveedor de claves con el cual desea establecer una conexión de confianza.

   Se muestra el servidor de claves (KMS) para el proveedor de claves.

4 En el menú desplegable **Establecer confianza**, seleccione **Hacer que KMS confíe en vCenter**.

5 Seleccione **Certificado de vCenter** y haga clic en **Siguiente**.

   El cuadro de diálogo Descargar certificado se rellena con el certificado raíz que vCenter Server utiliza para el cifrado. Este certificado se almacena en el almacén VECS.

   Nota No genere un certificado nuevo a menos que desee reemplazar los certificados existentes.

6 Copie el certificado en el portapapeles o descárguelo como un archivo.

7 Siga las instrucciones de su proveedor de KMS para cargar el certificado al KMS.

Pasos siguientes

Finalice la relación de confianza. Consulte Finalizar la configuración de confianza de un proveedor de claves estándar.

Usar la opción Cargar certificado y clave privada para establecer una conexión de confianza con el proveedor de claves estándar

Algunos proveedores de KMS requieren que se carguen el certificado del servidor KMS y la clave privada al sistema de vCenter Server.

Algunos proveedores de KMS generan un certificado y una clave privada para la conexión y los vuelven disponibles para el usuario. Una vez que haya cargado los archivos, el KMS establecerá una conexión de confianza con su instancia de vCenter Server.

Requisitos previos

- Solicite un certificado y una clave privada al proveedor de KMS. Los archivos son archivos X509 en formato PEM.

Procedimiento

1 Desplácese hasta vCenter Server.

2 Haga clic en **Configurar** y seleccione **Proveedores de claves** en **Seguridad**.

3 Seleccione el proveedor de claves con el cual desea establecer una conexión de confianza.

   Se muestra el servidor de claves (KMS) para el proveedor de claves.

4 En el menú desplegable **Establecer confianza**, seleccione **Hacer que KMS confíe en vCenter**.

5 Seleccione **Certificado y clave privada de KMS** y haga clic en **Siguiente**.

6 Pegue el certificado que recibió del proveedor de KMS en el cuadro de texto superior o haga clic en **Cargar un archivo** para cargar el archivo del certificado.

7 Pegue el archivo de claves en el cuadro de texto inferior o haga clic en **Cargar un archivo** para cargar el archivo de claves.

8 Haga clic en **Establecer confianza**.

Pasos siguientes

Finalice la relación de confianza. Consulte Finalizar la configuración de confianza de un proveedor de claves estándar.

Usar la opción Nueva solicitud de firma de certificado para establecer una conexión de confianza con el proveedor de claves estándar

Algunos proveedores de KMS requieren que vCenter Server genere una solicitud de firma del certificado (Certificate Signing Request, CSR) y la envíe al KMS. El KMS firma la CSR y devuelve el certificado firmado. El certificado firmado se puede cargar en vCenter Server.

El uso de la opción **Nueva solicitud de firma de certificado** es un proceso de dos pasos. Primero debe generar la CSR y enviarla al proveedor de KMS. A continuación, cargue el certificado firmado que recibió del proveedor de KMS a vCenter Server.

Procedimiento

1 Desplácese hasta vCenter Server.

2 Haga clic en **Configurar** y seleccione **Proveedores de claves** en **Seguridad**.

3 Seleccione el proveedor de claves con el cual desea establecer una conexión de confianza.

   Se muestra el servidor de claves (KMS) para el proveedor de claves.

4 En el menú desplegable **Establecer confianza**, seleccione **Hacer que KMS confíe en vCenter**.

5 Seleccione **Nueva solicitud de firma de certificado (CSR)** y haga clic en **Siguiente**.

6 En el cuadro de diálogo, copie el certificado completo del cuadro de texto en el portapapeles o descárguelo como un archivo.

   Use el botón **Generar nueva CSR** del cuadro de diálogo únicamente si desea generar una CSR de forma explícita.

7 Siga las instrucciones de su proveedor de KMS para enviar la CSR.

8 Cuando reciba el certificado firmado del proveedor de KMS, vuelva a hacer clic en **Proveedores de claves**, seleccione el proveedor de claves y, en el menú desplegable **Establecer confianza**, seleccione **Cargar certificado de CSR firmado**.

9 Pegue el certificado firmado en el cuadro de texto inferior o haga clic en **Cargar archivo** y cargue el archivo; luego, haga clic en **Aceptar**.

Pasos siguientes

Finalice la relación de confianza. Consulte Finalizar la configuración de confianza de un proveedor de claves estándar.

Finalizar la configuración de confianza de un proveedor de claves estándar

A menos que el cuadro de diálogo **Agregar proveedor de claves estándar** le haya solicitado confiar en el KMS, debe establecer la confianza explícitamente una vez finalizado el intercambio de certificados.

Es posible completar la instalación de confianza, es decir, hacer que vCenter Server confíe en el KMS, ya sea confiando en el KMS o cargando un certificado de KMS. Tiene dos opciones:

- Confiar en el certificado explícitamente por medio de la opción **Cargar certificado de KMS**.
- Cargar un certificado de hoja de KMS o el certificado de CA de KMS en vCenter Server por medio de la opción **Hacer que vCenter confíe en KMS**.

Nota Si carga el certificado de CA raíz o el certificado de CA intermedia, vCenter Server confía en todos los certificados que firma esa CA. Si desea obtener una seguridad más solida, cargue un certificado de hoja o un certificado de CA intermedia que controle el proveedor de KMS.

Procedimiento

1 Desplácese hasta vCenter Server.

2 Haga clic en **Configurar** y seleccione **Proveedores de claves** en **Seguridad**.

3 Seleccione el proveedor de claves con el cual desea establecer una conexión de confianza.

   Se muestra el servidor de claves (KMS) para el proveedor de claves.

4 Seleccione el KMS.

5 Seleccione una de las siguientes opciones en el menú desplegable **Establecer confianza**.

Opción	Acción
Hacer que vCenter confíe en KMS	En el cuadro de diálogo que aparece, haga clic en **Confiar**.
Cargar certificado de KMS	a En el cuadro de diálogo que aparece, pegue el certificado o haga clic en **Cargar un archivo** y desplácese hasta el archivo de certificado. b Haga clic en **Cargar**.

Configurar proveedores de claves independientes para diferentes usuarios

Puede configurar su entorno con diferentes proveedores de claves para distintos usuarios de la misma instancia de KMS. Tener varios proveedores de claves es útil, por ejemplo, si desea conceder a distintos departamentos de su empresa acceso a diferentes conjuntos de claves de cifrado.

Puede utilizar varios proveedores de claves para que el mismo KMS separe las claves. Tener distintos conjuntos de claves es esencial, por ejemplo, para casos de BU o clientes diferentes.

Nota No todos los proveedores de KMS admiten varios usuarios.

Requisitos previos

Establezca la conexión con el KMS.

Procedimiento

1 Cree dos usuarios con los correspondientes nombres de usuario y contraseñas, por ejemplo, C1 y C2, en el KMS.

2 Inicie sesión en vCenter Server y cree el primer proveedor de claves.

3 Cuando se le solicite un nombre de usuario y una contraseña, proporcione información que sea exclusiva para el primer usuario.

4 Cree un segundo proveedor de claves y agregue el mismo KMS, pero utilice el segundo nombre de usuario y contraseña (C2).

Resultados

Los dos proveedores de claves tienen conexiones independientes con el KMS y utilizan un conjunto diferente de claves.

Eliminar un proveedor de claves estándar

vSphere Client se puede utilizar para eliminar un proveedor de claves estándar de vCenter Server.

Después de eliminar un proveedor de claves estándar, las máquinas virtuales que tienen vTPM o que están cifradas siguen en ejecución. Si reinicia el host ESXi, sus máquinas virtuales cifradas entran en estado bloqueado. Después de cancelar el registro de estas máquinas virtuales, estas entran en un estado bloqueado cuando intenta volver a registrarlas. La única forma de desbloquear las máquinas virtuales es restaurar el proveedor de claves estándar anterior.

Requisitos previos

Privilegio necesario: **Operaciones criptográficas. Administrar servidores de claves**

Antes de eliminar un proveedor de claves estándar, vuelva a crear claves en las máquinas virtuales y los almacenes de datos cifrados que se cifraron con ese proveedor de claves en otro proveedor de claves. Consulte Cambiar la clave de una máquina virtual cifrada mediante vSphere Client.

Además, mantenga una copia de seguridad del proveedor de claves estándar en caso de que deba volver a crear claves en una máquina virtual cifrada después de eliminar el proveedor de claves.

Procedimiento

1. Inicie sesión en el sistema vCenter Server mediante vSphere Client.
2. Examine la lista de inventario y seleccione la instancia de vCenter Server.
3. Haga clic en **Configurar** y, en **Seguridad**, haga clic en **Proveedores de claves**.
4. Seleccione el proveedor de claves estándar que desea eliminar.
5. Haga clic en **Eliminar**.
6. Lea el mensaje de advertencia y deslice el control deslizante hasta llegar a la derecha.
7. Haga clic en **Eliminar**.

Resultados

El proveedor de claves estándar se elimina de vCenter Server.

Configurar y administrar el proveedor de claves nativo de vSphere

8

Para usar el proveedor de claves nativo de VMware vSphere® ™ en el entorno de vSphere se requiere algo de preparación. Después de configurar el proveedor de claves nativo de vSphere, puede crear módulos de plataforma de confianza virtuales (vTPM) en las máquinas virtuales.

Después de configurar el entorno para vSphere Native Key Provider, puede utilizar vSphere Client y la API para crear las vTPM. Si adquiere VMware vSphere® Enterprise Plus Edition™, también puede cifrar máquinas virtuales y discos virtuales, así como cifrar discos y máquinas virtuales existentes.



(Configurar una instancia de vSphere Native Key Provider)

Lea los siguientes temas a continuación:

Descripción general de vSphere Native Key Provider

In vSphere 7.0 Update 2 y versiones posteriores, puede usar vSphere Native Key Provider, que viene integrado, para habilitar tecnologías de cifrado como los TPM virtuales (vTPM).

vSphere Native Key Provider se incluye en todas las ediciones de vSphere y no requiere servidor de claves externo (también denominado en el sector servidor de administración de claves, KMS). También puede usar vSphere Native Key Provider para el cifrado de máquinas virtuales de vSphere, pero debe adquirir vSphere® Enterprise Plus Edition™ de VMware.

¿Qué es vSphere Native Key Provider?

Con un proveedor de claves estándar o un proveedor de claves de confianza, debe configurar un servidor de claves externo. En una configuración de proveedor de claves estándar, vCenter Server recupera las claves del servidor de claves externo y las distribuye a los hosts ESXi. En una configuración de proveedor de claves de confianza, (vSphere Trust Authority) los hosts ESXi de confianza recuperan las claves directamente.

Con vSphere Native Key Provider, ya no necesita un servidor de claves externo. vCenter Server genera una clave principal, denominada Clave de derivación de claves (Key Derivation Key, KDK), y la inserta en todos los hosts ESXi del clúster. A continuación, los hosts ESXi generan claves de cifrado de datos (incluso cuando no están conectados a vCenter Server) para habilitar la funcionalidad de seguridad, como vTPM. La funcionalidad vTPM se incluye en todas las ediciones vSphere. Para usar vSphere Native Key Provider para el cifrado de máquinas virtuales de vSphere, tiene que haber adquirido vSphere Enterprise Plus Edition. vSphere Native Key Provider puede coexistir con una infraestructura de servidor de claves existente.

vSphere Native Key Provider:

- Permite el uso de vTPM, cifrado de máquinas virtuales de vSphere y cifrado de datos en reposo de vSAN cuando no se necesita ni se desea tener un servidor de claves externo.
- Funciona únicamente con productos de infraestructura de VMware.
- No proporciona interoperabilidad externa, soporte de KMIP, módulos de seguridad de hardware u otras características que un servidor de claves externo tradicional de terceros puede ofrecer para el cumplimiento normativo o interoperabilidad. Si su organización requiere esta funcionalidad para productos y componentes que no son de VMware, instale un servidor de claves tradicional de terceros.
- Ayuda a solucionar las necesidades de las organizaciones que no pueden o no desean utilizar un servidor de claves externo.
- Mejora las prácticas de saneamiento de datos y reutilización de sistemas al facilitar el uso previo de tecnologías de cifrado en soportes difíciles de sanear, como las memorias flash y las unidades SSD.
- Proporciona una ruta de acceso de transición entre proveedores de claves. vSphere Native Key Provider es compatible con el proveedor de claves estándar de VMware y con el proveedor de claves de confianza vSphere Trust Authority.
- Funciona con varios sistemas vCenter Server mediante una configuración de Enhanced Linked Mode o una configuración de vCenter Server High Availability.
- Se puede utilizar para habilitar vTPM en todas las ediciones de vSphere y cifrar máquinas virtuales con la compra de vSphere Enterprise Plus Edition que incluye cifrado de máquinas virtuales de vSphere. El cifrado de máquinas virtuales de vSphere funciona con vSphere Native Key Provider de la misma manera que con los proveedores de claves estándar y de confianza de VMware.

- Se puede utilizar para habilitar el cifrado de datos en reposo de vSAN con el uso de una licencia de vSAN adecuada.
- Puede utilizar un módulo de plataforma de confianza (Trusted Platform Module, TPM) 2.0 para aumentar la seguridad cuando se instala en un host ESXi. También puede configurar vSphere Native Key Provider para que solo esté disponible para los hosts en los que hay un TPM 2.0 instalado. Si utiliza un TPM, debe ser TPM 2.0. vSphere Native Key Provider no admite TPM 1.2.

Nota Un host ESXi no requiere un TPM 2.0 para usar una instancia de vSphere Native Key Provider. No obstante un TPM 2.0 sí brinda seguridad mejorada.

Al igual que con todas las soluciones de seguridad, tenga en cuenta el diseño del sistema, las consideraciones de implementación y las ventajas del uso de vSphere Native Key Provider. Por ejemplo, la persistencia de claves de ESXi evita la dependencia de que un servidor de claves esté siempre disponible. Sin embargo, debido a que la persistencia de claves almacena la información criptográfica de vSphere Native Key Provider en los hosts agrupados en clúster, seguirá estando en situación de riesgo si los agentes malintencionados roban los propios hosts ESXi. Dado que los entornos difieren, evalúe e implemente los controles de seguridad de acuerdo con las necesidades normativas y de seguridad de su organización, los requisitos operativos y la tolerancia al riesgo.

Para obtener más información general sobre vSphere Native Key Provider, consulte https://core.vmware.com/native-key-provider.

Requisitos de vSphere Native Key Provider

Para usar vSphere Native Key Provider, debe:

- Asegúrese de que el sistema vCenter Server y los hosts ESXi ejecuten vSphere 7.0 Update 2 o una versión posterior.
- Configure los hosts ESXi en un clúster.
- Si bien no es necesario, como práctica recomendada, utilice hosts ESXi que sean lo más idénticos posible, incluidos los TPM. La administración de clústeres y la habilitación de funciones son mucho más sencillas cuando los hosts del clúster son idénticos.
- Configure la copia de seguridad y la restauración basadas en archivos de vCenter Server, y almacene las copias de seguridad de forma segura, ya que contienen la clave de derivación de claves. Consulte el tema sobre copia de seguridad y restauración de vCenter Server en la documentación de *Instalar y configurar vCenter Server*.

Para realizar cifrado de máquinas virtuales de vSphere o cifrado de vSAN mediante vSphere Native Key Provider, debe adquirir la edición de los productos que contengan la licencia adecuada.

vSphere Native Key Provider y Enhanced Linked Mode

Puede configurar un vSphere Native Key Provider único que se pueda compartir entre sistemas vCenter Server dispuestos en una configuración de Enhanced Linked Mode. Los pasos de alto nivel en este escenario son los siguientes:

1 Crear el vSphere Native Key Provider en uno de los sistemas vCenter Server

2 Hacer una copia de seguridad de vSphere Native Key Provider en el vCenter Server en el que se creó

3 Exportar el vSphere Native Key Provider

4 Restaurar el vSphere Native Key Provider a otros sistemas vCenter Server existentes en la configuración de Enhanced Link Mode (consulte Restaurar un vSphere Native Key Provider mediante el vSphere Client)

Privilegios de vSphere Native Key Provider

Al igual que los proveedores de claves estándar y de confianza, vSphere Native Key Provider utiliza los privilegios **Cryptographer***. Además, vSphere Native Key Provider utiliza el privilegio **Cryptographer.ReadKeyServersInfo**, que es específico de él, para enumerar las instancias de vSphere Native Key Provider. Consulte Privilegios de operaciones de cifrado.

Alarmas de vSphere Native Key Provider

Debe realizar una copia de seguridad de vSphere Native Key Provider. Cuando no se realiza una copia de seguridad de vSphere Native Key Provider, vCenter Server genera una alarma. Después de que haga una copia de seguridad de la instancia de vSphere Native Key Provider para la que se generó una alarma, vCenter Server restablecerá la alarma. De forma predeterminada, vCenter Server comprueba una vez al día que las instancias de vSphere Native Key Provider tengan una copia de seguridad. Puede cambiar el intervalo de comprobación modificando la opción `vpxd.KMS.backupCheckInterval`.

Comprobación de corrección periódica de vSphere Native Key Provider

vCenter Server comprueba periódicamente que la configuración de vSphere Native Key Provider en vCenter Server coincida con la de los hosts ESXi. Cuando cambia el estado de un host, por ejemplo, cuando agrega un host al clúster, la configuración del proveedor de claves en el clúster se diferencia de la configuración en el host. Si la configuración (keyID) es diferente en el host, vCenter Server actualiza automáticamente la configuración del host. No se requiere intervención manual.

De forma predeterminada, vCenter Server comprueba la configuración cada cinco minutos. Puede modificar el intervalo mediante la opción `vpxd.KMS.remediationInterval`.

Usar vSphere Native Key Provider con un sitio de recuperación ante desastres

Puede utilizar vSphere Native Key Provider con un sitio de recuperación ante desastres de copia de seguridad. La importación de la copia de seguridad de vSphere Native Key Provider desde la instancia principal de vCenter Server a la instancia de copia de seguridad de vCenter Server en el sitio de recuperación ante desastres permite que ese clúster descifre y ejecute las máquinas virtuales cifradas.

Pruebe siempre su solución de recuperación ante desastres. Nunca asuma que su solución funciona sin intentar una recuperación. Asegúrese de que una copia de seguridad de vSphere Native Key Provider también esté disponible para el sitio de recuperación ante desastres.

Funciones no compatibles en vSphere Native Key Provider

Actualmente, vSphere Native Key Provider no admite lo siguiente:

- Cifrado de disco de primera clase (First Class Disk, FCD)

Migrar máquinas virtuales mediante vSphere Native Key Provider en sistemas vCenter Server no vinculados

Los pasos de alto nivel para migrar una máquina virtual, ya sea cifrada o habilitada con un vTPM a través de vSphere Native Key Provider, de un sistema vCenter Server no vinculado a otro, incluyen:

1 Restaurar el vSphere Native Key Provider al sistema vCenter Server al que se va a migrar.

2 Migración de la máquina virtual mediante vMotion.

Flujos de procesos de vSphere Native Key Provider

Comprender los flujos de procesos de vSphere Native Key Provider es esencial para aprender a configurar y administrar vSphere Native Key Provider.

Puede usar vSphere Native Key Provider, que viene integrado, para encender los TPM virtuales basados en cifrado (vTPM). vSphere Native Key Provider se incluye en todas las ediciones de vSphere y no requiere un servidor de claves externo (KMS). Para usar vSphere Native Key Provider para el cifrado de máquinas virtuales de vSphere, debe adquirir la edición vSphere Enterprise+.

Configurar vSphere Native Key Provider

La configuración de vSphere Native Key Provider implica estas operaciones básicas:

1 Un usuario con los privilegios administrativos adecuados utiliza vSphere Client para crear un vSphere Native Key Provider en un vCenter Server.

2 A continuación, vCenter Server configura vSphere Native Key Provider para todos los clústeres de hosts ESXi.

En este paso, vCenter Server inserta una clave principal en todos los hosts ESXi del clúster. Del mismo modo, si actualiza o elimina un proveedor de claves nativo de vSphere, el cambio se inserta en los hosts del clúster.

3 Los usuarios con los privilegios criptográficos adecuados crean vTPM y máquinas virtuales cifradas (siempre y cuando haya adquirido la edición vSphere Enterprise+).

   Consulte Capítulo 10 Usar el cifrado en el entorno de vSphere y Capítulo 11 Proteger las máquinas virtuales con el módulo de plataforma de confianza virtual.

Flujo del proceso de cifrado del proveedor de claves nativo de vSphere

Para comprender cómo interactúan los diferentes componentes para realizar una tarea de cifrado con vSphere Native Key Provider, consulte Flujo del proceso de cifrado de vSphere Native Key Provider.

Configurar un vSphere Native Key Provider

Se requiere un proveedor de claves para realizar tareas de cifrado. Puede usar la instancia de vSphere Client para configurar vSphere Native Key Provider en vCenter Server.

vSphere 7.0 Update 2 y las versiones posteriores incluyen un proveedor de claves llamado vSphere Native Key Provider. vSphere Native Key Provider habilita la funcionalidad relacionada con el cifrado sin necesidad de un servidor de claves externo (KMS). Inicialmente, vCenter Server no está configurado con un vSphere Native Key Provider. Debe configurar manualmente un vSphere Native Key Provider.

Un host ESXi no requiere un TPM 2.0 para usar una instancia de vSphere Native Key Provider. No obstante un TPM 2.0 sí brinda seguridad mejorada.

Nota Cuando se configura vSphere Native Key Provider, los proveedores de claves están disponibles en todos los clústeres para los vCenter Server en los que se configuran. Como resultado, todos los hosts asociados a la vCenter Server tendrán acceso a todos los vSphere Native Key Providers que configure.

Requisitos previos

Privilegio necesario: **Operaciones criptográficas. Administrar servidores de claves**

Procedimiento

1 Inicie sesión en el sistema vCenter Server mediante vSphere Client.

2 Examine la lista de inventario y seleccione la instancia de vCenter Server.

3 Haga clic en **Configurar** y, en **Seguridad**, haga clic en **Proveedores de claves**.

4 Haga clic en **Agregar** a continuación, haga clic en **Agregar proveedor de claves nativo**.

5 Introduzca un nombre para el vSphere Native Key Provider.

   Cada proveedor de claves lógico, independientemente de su tipo (proveedor de claves estándar, de confianza y nativo), debe tener un nombre único en todos los sistemas vCenter Server.

   Para obtener más información, consulte Nomenclatura de proveedor de claves.

6 Si desea que a esta instancia de vSphere Native Key Provider solo la utilicen hosts con TPM 2.0, seleccione la casilla de verificación **Usar proveedor de claves solo con hosts ESXi con protección de TPM**.

   Si se habilita, la instancia de vSphere Native Key Provider solo está disponible en hosts con un TPM 2.0.

7 Haga clic en **Agregar proveedor de claves**.

   Nota Todos los hosts de ESXi en clúster de un centro de datos tardan unos cinco minutos en obtener el proveedor de claves y en que el vCenter Server actualice su memoria caché. Debido a la forma en que se propaga la información, es posible que deba esperar unos minutos para utilizar el proveedor de claves para operaciones de claves en algunos de los hosts.

Resultados

Se agrega el vSphere Native Key Provider y aparece en el panel **Proveedor de claves**. En este punto, no se hace la copia de seguridad del vSphere Native Key Provider. Debe realizar una copia de seguridad del vSphere Native Key Provider para poder utilizarlo.

Pasos siguientes

Consulte Hacer una copia de seguridad de vSphere Native Key Provider.

Hacer una copia de seguridad de vSphere Native Key Provider

En caso de que deba restaurar la configuración del proveedor de claves, se requiere la copia de seguridad de un vSphere Native Key Provider como parte de un escenario de recuperación ante desastres. Puede utilizar la vSphere Client, PowerCLI o API para realizar una copia de seguridad del vSphere Native Key Provider.

Se hace una copia de seguridad del vSphere Native Key Provider como parte de la copia de seguridad basada en archivos vCenter Server. Sin embargo, debe realizar una copia de seguridad del vSphere Native Key Provider al menos una vez antes de poder utilizarlo. Cuando se crea un vSphere Native Key Provider, no se hace una copia de seguridad de él.

Se necesita una copia de seguridad en caso de que deba restaurar la configuración. Para restaurar un vSphere Native Key Provider, consulte Restaurar un vSphere Native Key Provider mediante el vSphere Client.

Mantenga el archivo de copia de seguridad en una ubicación segura. Puede proteger con contraseña la copia de seguridad cuando la cree. El archivo de copia de seguridad tiene el formato PKCS#12.

vCenter Server crea una alarma si no hay una copia de seguridad de un vSphere Native Key Provider. Puede confirmar la alarma, pero esta vuelve a aparecer cada 24 horas hasta que haya hecho una copia de seguridad del vSphere Native Key Provider.

Requisitos previos

Privilegio necesario: **Operaciones criptográficas. Administrar servidores de claves**

Nota En una configuración de Enhanced Link Mode, debe realizar la copia de seguridad en vCenter Server al que pertenece el proveedor de claves.

Procedimiento

1 Inicie sesión en el sistema vCenter Server mediante vSphere Client.

2 Examine la lista de inventario y seleccione la instancia de vCenter Server.

3 Haga clic en **Configurar** y, en **Seguridad**, haga clic en **Proveedores de claves**.

4 Seleccione el vSphere Native Key Provider del que desea hacer una copia de seguridad.

   Aparece el estado "Sin copia de seguridad" para los proveedores de claves de los que no se ha hecho una copia de seguridad.

5 Haga clic **Hacer copia de seguridad**.

6 Para proteger con contraseña la copia de seguridad, active la casilla **Proteger los datos del proveedor de claves nativo con una contraseña** .

   a Introduzca una contraseña y guárdela en una ubicación segura.

   b Active la casilla **He guardado la contraseña en un lugar seguro**, indicando que ha guardado la contraseña en un lugar seguro.

7 Haga clic en **Hacer copia de seguridad del proveedor de claves**.

   El archivo de copia de seguridad tiene el formato PKCS#12.

8 Guarde el archivo de copia de seguridad en una ubicación segura.

Resultados

El estado del vSphere Native Key Provider cambia de Sin copia de seguridad, a Advertencia, a Activo. La advertencia indica que el vCenter Server aún está insertando la información en todos los hosts ESXi del centro de datos. Activo significa que la información se ha insertado a todos los hosts.

Pasos siguientes

Para agregar los vTPM a máquinas virtuales, consulte Capítulo 11 Proteger las máquinas virtuales con el módulo de plataforma de confianza virtual. Para cifrar máquinas virtuales, consulte Capítulo 10 Usar el cifrado en el entorno de vSphere.

Recuperar un proveedor de claves nativo de vSphere

Puede recuperar el proveedor de claves nativo de vSphere a través de la vSphere Client o desde la copia de seguridad vCenter Server Appliance.

Cuando sea necesario, puede recuperar un proveedor de claves nativo de vSphere de las siguientes maneras.

1 Si no necesita reconstruir el vCenter Server Appliance, utilice el vSphere Client para restaurar el proveedor de claves. Consulte Restaurar un vSphere Native Key Provider mediante el vSphere Client.

2 Si debe volver a construir la vCenter Server Appliance, debe restaurar el proveedor de claves desde la copia de seguridad vCenter Server Appliance. Cuando se realiza una copia de seguridad vCenter Server Appliance, se guarda el proveedor de claves nativo. Consulte https://blogs.vmware.com/vsphere/2018/05/vcenter-server-appliance-6-7-file-based-backup-and-restore-walkthroughs.html para obtener información sobre cómo restaurar los vCenter Server Appliance de la copia de seguridad.

Restaurar un vSphere Native Key Provider mediante el vSphere Client

Puede usar el vSphere Client para restaurar el vSphere Native Key Provider.

Puede restaurar un vSphere Native Key Provider en caso de que se haya eliminado accidentalmente o si debe realizar una recuperación ante desastres.

Al restaurar un vSphere Native Key Provider, no es necesario que vuelva a realizar una copia de seguridad del proveedor de claves. La copia de seguridad inicial es suficiente. Continúe para mantener el archivo de copia de seguridad en una ubicación segura.

Nota También puede utilizar esta tarea para configurar vSphere Native Key Provider para sistemas vCenter Server en una configuración de Enhanced Linked Mode. Después de crear el vSphere Native Key Provider en un sistema vCenter Server en la configuración de Enhanced Linked Mode, utilice la función **Restaurar** para importar el archivo de clave cifrado en los otros sistemas vCenter Server conectados a ELM.

Requisitos previos

- Privilegio necesario: **Operaciones criptográficas. Administrar servidores de claves**
- El archivo de copia de seguridad del proveedor de claves.

- La contraseña del archivo del proveedor de claves, si introdujo una cuando escribió una copia de seguridad del proveedor de claves.

Procedimiento

1 Inicie sesión en el sistema vCenter Server mediante vSphere Client.

2 Examine la lista de inventario y seleccione la instancia de vCenter Server.

3 Haga clic en **Configurar** y, en **Seguridad**, haga clic en **Proveedores de claves**.

4 Seleccione el vSphere Native Key Provider y haga clic en **Restaurar**.

5 Desplácese hasta la ubicación del archivo y seleccione el archivo de clave cifrada de la copia de seguridad.

   El archivo se guardó en formato PKCS#12.

6 (opcional) Si el archivo está protegido con contraseña, introduzca la contraseña.

7 Haga clic en **Siguiente**.

8 (opcional) Si decidió utilizar este proveedor de claves solo con hosts ESXi protegidos por TPM, seleccione la casilla de verificación.

9 Haga clic en **Finalizar**.

Resultados

El vSphere Native Key Provider se importa en vCenter Server. Para utilizar el vSphere Native Key Provider para las tareas de cifrado, asegúrese de seleccionarlo primero en el panel **Proveedor de claves** y haga clic en **Establecer como valor predeterminado**.

Actualizar un vSphere Native Key Provider

Como parte de sus planes de rotación de claves regulares, puede utilizar PowerCLI para actualizar un vSphere Native Key Provider.

Si tiene una directiva para la rotación de claves, puede actualizar el vSphere Native Key Provider y regenerar claves en las máquinas virtuales que cifró con ese proveedor de claves. Debe usar PowerCLI para actualizar el vSphere Native Key Provider. También puede regenerar claves para las máquinas virtuales cifradas sin actualizar el proveedor de claves. En este caso, solo se cambian las claves de la máquina virtual. Para regenerar la clave de una máquina virtual, consulte Cambiar la clave de una máquina virtual cifrada mediante vSphere Client.

Requisitos previos

- Privilegio necesario: **Operaciones criptográficas. Administrar servidores de claves**
- PowerCLI 12.3.0

Procedimiento

1 En una sesión de PowerCLI, ejecute el cmdlet `Connect-VIServer` para conectarse como usuario administrador al vCenter Server donde configuró el vSphere Native Key Provider que desea actualizar.

```
Connect-VIServer -server VC_ip_address -User admin_user -Password 'password'
```

2 Para obtener los nombres del vSphere Native Key Provider, ejecute el cmdlet `Get-KeyProvider` con el parámetro `Type` opcional.

```
Get-KeyProvider -Type NativeKeyProvider
```

3 Para actualizar el proveedor de claves, ejecute el cmdlet `Set-KeyProvider` y especifique el nombre y el GUID del proveedor de claves.

Puede generar un GUID para utilizar mediante la ejecución del cmdlet `New-Guid`.

```
Set-KeyProvider -KeyProvider KeyProvider_name -KeyId Guid
```

Se muestra una advertencia acerca de la copia de seguridad de la configuración.

4 Para crear una copia de seguridad del proveedor de claves, ejecute el cmdlet `Export-KeyProvider`.

```
Export-KeyProvider -KeyProvider KeyProvider_name -FilePath path_file_name
```

También puede realizar una copia de seguridad del proveedor de claves mediante el vSphere Client. Consulte Hacer una copia de seguridad de vSphere Native Key Provider.

Resultados

Cuando se actualiza un proveedor de claves, su estado cambia a Sin copia de seguridad. Después de realizar una copia de seguridad del proveedor de claves, su estado cambia a Activo.

Eliminar un proveedor de claves nativo de vSphere

vSphere Client se puede utilizar para eliminar un vSphere Native Key Provider en vCenter Server.

Después de eliminar un proveedor de claves nativo de vSphere, las máquinas virtuales que tienen vTPM o que están cifradas siguen en ejecución. Si reinicia el host ESXi, sus máquinas virtuales cifradas entran en estado bloqueado. Después de cancelar el registro de estas máquinas virtuales, estas entran en un estado bloqueado cuando intenta volver a registrarlas. La única forma de desbloquear las máquinas virtuales es restaurar el proveedor de claves nativo de vSphere anterior.

Requisitos previos

Privilegio necesario: **Operaciones criptográficas. Administrar servidores de claves**

Antes de eliminar un proveedor de claves nativo de vSphere, vuelva a crear claves en las máquinas virtuales y los almacenes de datos cifrados que se cifraron con ese proveedor de claves en otro proveedor de claves. Consulte Cambiar la clave de una máquina virtual cifrada mediante vSphere Client.

Además, mantenga una copia de seguridad de vSphere Native Key Provider en caso de que deba volver a crear claves en una máquina virtual cifrada después de eliminar el proveedor de claves.

Procedimiento

1. Inicie sesión en el sistema vCenter Server mediante vSphere Client.
2. Examine la lista de inventario y seleccione la instancia de vCenter Server.
3. Haga clic en **Configurar** y, en **Seguridad**, haga clic en **Proveedores de claves**.
4. Seleccione el proveedor de claves que desea eliminar.
5. Haga clic en **Eliminar**.
6. Lea el mensaje de advertencia y deslice el control deslizante hasta llegar a la derecha.
7. Haga clic en **Eliminar**.

Resultados

El proveedor de claves nativo de vSphere se elimina del vCenter Server.

vSphere Trust Authority

9

Con vSphere 7.0 y versiones posteriores, puede aprovechar VMware® vSphere Trust Authority™. vSphere Trust Authority es una tecnología de base que mejora la seguridad de la carga de trabajo. vSphere Trust Authority establece un mayor nivel de confianza en la organización al asociar la raíz de confianza del hardware de un host ESXi a la propia carga de trabajo.

Lea los siguientes temas a continuación:

Conceptos y funciones de vSphere Trust Authority

vSphere Trust Authority protege el SDDC contra ataques malintencionados mediante la ampliación de la confiabilidad de una base informática de confianza a la infraestructura informática completa de su organización. vSphere Trust Authority utiliza la atestación remota y el acceso controlado para las capacidades de cifrado avanzadas.

vSphere Trust Authority es un conjunto de servicios que satisface los requisitos de alta seguridad. Con vSphere Trust Authority, puede configurar y mantener una infraestructura segura. Puede garantizar que las cargas de trabajo confidenciales se ejecuten solo en hosts ESXi en los que se haya comprobado que se arrancó software auténtico.

Cómo vSphere Trust Authority protege su entorno

Los servicios de vSphere Trust Authority se configuran para atestar los hosts ESXi, los cuales luego pueden realizar operaciones criptográficas de confianza.

vSphere Trust Authority utiliza la atestación remota para que los hosts ESXi demuestren la autenticidad de su software arrancado. La atestación verifica que los hosts ESXi ejecutan software VMware auténtico o software de socio firmado por VMware. La atestación depende de las mediciones que provienen de un chip de módulo de plataforma de confianza (Trusted Platform Module, TPM) 2.0 instalado en el host ESXi. En vSphere Trust Authority, una instancia de ESXi puede acceder a las claves de cifrado y realizar operaciones criptográficas solo después de que se haya atestado.

Glosario de vSphere Trust Authority

vSphere Trust Authority introduce términos y definiciones específicos que resulta importante comprender.

Tabla 9-1. Glosario de vSphere Trust Authority

Término	Definición
VMware vSphere® Trust Authority™	Especifica un conjunto de servicios que habilita una infraestructura de confianza. Es responsable de garantizar que los hosts ESXi ejecuten software de confianza y de que solo se liberen claves de cifrado en hosts ESXi de confianza.
Componentes de vSphere Trust Authority	Los componentes de vSphere Trust Authority son los siguientes: ■ Servicio de atestación ■ Servicio de proveedor de claves
Servicio de atestación	Atesta el estado de un host ESXi remoto. Utiliza TPM 2.0 para establecer una raíz de confianza del hardware y comprueba las mediciones de software con una lista de versiones de ESXi aprobadas por el administrador.
Servicio de proveedor de claves	Encapsula uno o varios servidores de claves y expone proveedores de claves de confianza que se pueden especificar al cifrar máquinas virtuales. Actualmente, los servidores de claves se limitan al protocolo KMIP.
Infraestructura de confianza	Una infraestructura de confianza consta de lo siguiente: ■ Una instancia de vCenter Server de Trust Authority ■ Una instancia devCenter Server de carga de trabajo ■ Al menos un clúster de vSphere Trust Authority (configurado como parte de vCenter Server de Trust Authority) ■ Al menos un clúster de confianza (configurado como parte de vCenter Server de carga de trabajo) ■ Máquinas virtuales de carga de trabajo cifradas en ejecución en el clúster de confianza ■ Al menos un servidor de administración de claves que cumpla con KMIP **Nota** Debe utilizar sistemas vCenter Server independientes para el clúster de Trust Authority y el clúster de confianza.
Clúster de Trust Authority	Consiste en un clúster de vCenter Server de hosts ESXi que ejecutan componentes de vSphere Trust Authority (el servicio de atestación y el servicio de proveedor de claves).
Host de Trust Authority	Un host ESXi que ejecuta componentes de vSphere Trust Authority (el servicio de atestación y el servicio de proveedor de claves).
Clúster de confianza	Consiste en un clúster de vCenter Server de hosts ESXi de confianza que el clúster de Trust Authority atesta de forma remota. Aunque no es estrictamente obligatorio, un servicio de proveedor de claves configurado aumenta enormemente el valor que proporciona un clúster de confianza.
Host de confianza	Un host ESXi cuyo software ha sido validado por el servicio de atestación del clúster de Trust Authority. Este host ejecuta máquinas virtuales de carga de trabajo que se pueden cifrar mediante proveedores de claves publicados por el servicio de proveedor de claves del clúster de Trust Authority.
Cifrado de vSphere para máquinas virtuales	El cifrado de máquinas virtuales de vSphere puede crear máquinas virtuales cifradas y cifrar las máquinas virtuales existentes. El cifrado de máquinas virtuales de vSphere se introdujo en vSphere 6.5. Consulte Claves de cifrado y proveedores de claves de vSphere para conocer las diferencias en cómo los proveedores de claves gestionan las claves de cifrado.

Tabla 9-1. Glosario de vSphere Trust Authority (continuación)

Término	Definición
Proveedor de claves de confianza	Un proveedor de claves que encapsula una única clave de cifrado en un servidor de claves. El acceso a la clave de cifrado requiere que el servicio de atestación confirme que el software de ESXi se verificó en el host de confianza.
Proveedor de claves estándar	Un proveedor de claves que obtiene las claves de cifrado directamente de un servidor de claves y distribuye claves a los hosts necesarios en un centro de datos. En vSphere, anteriormente se conocía como clúster de KMS.
Servidor de claves	Un servidor de administración de claves (Key Management Server, KMS) de KMIP que está asociado a un proveedor de claves.
vCenter Server de carga de trabajo	El vCenter Server que administra y se utiliza para configurar uno o varios clústeres de confianza.

Conceptos básicos de vSphere Trust Authority

Con vSphere Trust Authority, se puede realizar lo siguiente:

- Proporcionar hosts ESXi con una raíz de hardware de confianza y capacidades de atestación remota
- Restringir la administración de claves de cifrado mediante la liberación de claves solo a hosts ESXi atestados
- Crear un entorno administrativo más seguro para administrar la confianza
- Centralizar la administración de varios servidores de claves
- Continuar realizando operaciones criptográficas en máquinas virtuales, pero con un nivel mejorado de administración de claves de cifrado

En vSphere 6.5 y 6.7, el cifrado de máquinas virtuales depende de vCenter Server para obtener claves de cifrado de un servidor de claves e insertarlas en los hosts ESXi según corresponda. vCenter Server autentifica con el servidor de claves utilizando los certificados del cliente y del servidor, que se almacenan en VMware Endpoint Certificate Store (VECS). Las claves de cifrado que se envían desde el servidor de claves pasan por la memoria de vCenter Server a los hosts ESXi requeridos (con cifrado de datos proporcionado por TLS a través de la conexión). Además, vSphere depende de las comprobaciones de privilegios en vCenter Serverpara validar los permisos de los usuarios y aplicar las restricciones de acceso al servidor de claves. Aunque esta arquitectura es segura, no soluciona la posibilidad de que se produzca un riesgo para vCenter Server, que haya un administrador de vCenter Server malintencionado o que se presente un error de administración o de configuración que pueda provocar pérdidas o robo de secretos.

En vSphere 7.0 y versiones posteriores, vSphere Trust Authority soluciona estos problemas. Puede crear una base informática de confianza, que consta de un conjunto seguro y manejable de hosts ESXi. vSphere Trust Authority implementa un servicio de atestación remoto para los hosts ESXi en los que desea confiar. Además, vSphere Trust Authority mejora la compatibilidad con la atestación de TPM 2.0 (agregada a vSphere a partir de la versión 6.7), para implementar restricciones de acceso en las claves de cifrado y, así, proteger mejor los secretos de carga

de trabajo de las máquinas virtuales. Además, vSphere Trust Authority solo permite que administradores de Trust Authority autorizados configuren los servicios de vSphere Trust Authority y los hosts de Trust Authority. El administrador de Trust Authority puede ser el mismo usuario que el usuario administrador de vSphere, o bien, uno independiente.

Al final, vSphere Trust Authority permite ejecutar las cargas de trabajo en un entorno más seguro y protegido mediante lo siguiente:

- Detectar alteraciones
- No permitir cambios no autorizados
- Evitar malware y modificaciones
- Limitar que las cargas de trabajo confidenciales se ejecuten solo en una pila de hardware y software seguro y verificado

Arquitectura de vSphere Trust Authority

En la siguiente figura, se muestra una vista simplificada de la arquitectura de vSphere Trust Authority.

Figura 9-1. Arquitectura de vSphere Trust Authority

En esta figura:

1 Sistemas vCenter Server

Sistemas vCenter Server independientes administran el clúster de Trust Authority y los clústeres de confianza.

2 Clúster de Trust Authority

Consta de los hosts ESXi que ejecutan los componentes de vSphere Trust Authority.

3 Servidores de claves

Almacenan claves de cifrado que utiliza el servicio de proveedor de claves cuando se realizan operaciones de cifrado. Los servidores de claves son externos a vSphere Trust Authority.

4 Clústeres de confianza

Consta de los hosts de confianza ESXi que se han atestado de forma remota con un TPM y que ejecutan cargas de trabajo cifradas.

5 Administrador de Trust Authority

Administrador que es miembro del grupo TrustedAdmins de vCenter Server y que configura la infraestructura de confianza.

vSphere Trust Authority permite que haya flexibilidad en el modo en que se designan los administradores de Trust Authority. Los administradores de Trust Authority de la figura pueden ser usuarios independientes. También es posible que los administradores de Trust Authority sean el mismo usuario, mediante credenciales vinculadas a través de los sistemas vCenter Server. En este caso, es el mismo usuario y el mismo grupo TrustedAdmins.

6 Administrador de máquinas virtuales

Administrador al que se han otorgado privilegios para administrar las máquinas virtuales de carga de trabajo cifradas en los hosts de confianza.

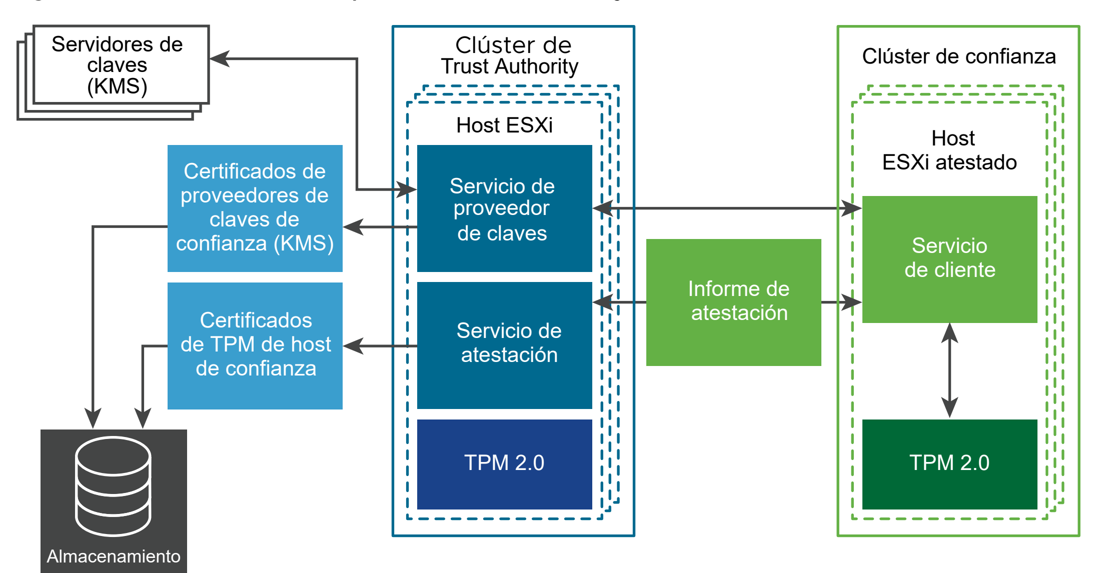
Infraestructura de confianza de vSphere Trust Authority

Los servicios de vSphere Trust Authority, al menos un servidor de claves externo compatible con KMIP, los sistemas de vCenter Server y los hosts ESXi contribuyen a la infraestructura de confianza.

Descripción de una infraestructura de confianza

Una infraestructura de confianza se compone como mínimo de un clúster de vSphere Trust Authority, un clúster de confianza y un servidor de claves externo compatible con KMIP. Cada clúster contiene hosts ESXi que ejecutan servicios de vSphere Trust Authority específicos, como se muestra en la siguiente figura.

Figura 9-2. Servicios de vSphere Trust Authority



La configuración del clúster de Trust Authority ofrece dos servicios:

- Servicio de atestación
- Servicio de proveedor de claves

Cuando se configura vSphere Trust Authority, los hosts ESXi del clúster de confianza se comunican con el servicio de atestación. El servicio de proveedor de claves se interpone entre los hosts de confianza y uno o varios proveedores de claves de confianza.

Nota Actualmente, los hosts ESXi del clúster de Trust Authority no requieren un TPM. Sin embargo, como práctica recomendada, considere la posibilidad de instalar nuevos hosts ESXi con TPM.

Qué es el servicio de atestación de vSphere Trust Authority

El servicio de atestación genera un documento firmado que contiene aserciones en las que se describe el estado binario y de configuración de los hosts ESXi remotos en el clúster de confianza. El servicio de atestación acredita el estado de los hosts ESXi que utilizan un chip del módulo de plataforma de confianza (Trusted Platform Module, TPM) 2.0 como base para la medición y la generación de informes de software. El TPM del host ESXi remoto mide la pila de software y envía los datos de configuración al servicio de atestación. El servicio de atestación verifica que la firma de medición de software se pueda atribuir a una clave de aprobación (EK) de TPM de confianza configurada previamente. El servicio de atestación también garantiza que la medición de software coincida con una imagen de un conjunto de imágenes de ESXi previamente designadas. El servicio de atestación firma un token web de JSON (JWT) que envía al host ESXi, lo que proporciona las aserciones sobre la identidad, la validez y la configuración del host ESXi.

Descripción del servicio de proveedor de claves de vSphere Trust Authority

Con el servicio de proveedor de claves, ya no es necesario que vCenter Server y los hosts ESXi requieran credenciales de servidor de claves directas. En vSphere Trust Authority, para que un host ESXi tenga acceso a una clave de cifrado, debe autenticarse con el servicio de proveedor de claves.

Para que el servicio de proveedor de claves se conecte a un servidor de claves, el administrador de Trust Authority debe establecer una configuración de confianza. En la mayoría de los servidores compatibles con KMIP, una configuración de confianza implica configurar certificados de cliente y servidor.

Para garantizar que las claves solo publiquen en hosts ESXi de confianza, el servicio de proveedor de claves actúa como guardián de los servidores principales. El servicio de proveedor de claves oculta las especificaciones del servidor de claves del resto de la pila de software en el centro de datos mediante un proveedor de claves de confianza. Cada proveedor de claves de confianza tiene una sola clave de cifrado principal configurada y hace referencia a uno o varios servidores de claves. El servicio de proveedor de claves puede tener varios proveedores de claves de confianza configurados. Por ejemplo, es posible que desee tener un proveedor de claves de confianza independiente para cada departamento de una organización. Cada proveedor de claves de confianza utiliza una clave principal diferente, pero puede hacer referencia al mismo servidor de claves de respaldo.

Después de crear un proveedor de claves de confianza, el servicio de proveedor de claves puede aceptar solicitudes de los hosts ESXi de confianza para ejecutar operaciones criptográficas en ese proveedor de claves de confianza.

Cuando un host ESXi de confianza solicita operaciones frente a un proveedor de claves de confianza, el servicio del proveedor de claves garantiza que se certifique el host ESXi que está intentando obtener la clave de cifrado. Después de pasar todas las comprobaciones, el host ESXi de confianza recibe claves de cifrado del servicio de proveedor de claves.

Qué puertos utiliza vSphere Trust Authority

Los servicios de vSphere Trust Authority escuchan conexiones detrás del proxy inverso del host ESXi. Todas las comunicaciones se producen a través de HTTPS en el puerto 443.

Qué son los hosts vSphere Trust Authority de confianza

Los hosts ESXi de confianza están configurados para usar proveedores de claves de confianza a fin de realizar operaciones de cifrado. Los hosts ESXi de confianza realizan operaciones clave al comunicarse con el servicio de proveedor de claves y el servicio de atestación. Para las operaciones de autenticación y autorización, los hosts ESXi de confianza utilizan un token que se obtiene del servicio de atestación. Para obtener un token válido, el host ESXi de confianza debe atestiguarse correctamente en el servicio de atestación. El token contiene ciertas notificaciones que se utilizan a fin de decidir si el host ESXi de confianza tiene autorización para acceder a un proveedor de claves de confianza.

Requisitos de vSphere Trust Authority y el servidor de claves

vSphere Trust Authority requiere el uso de al menos un servidor de claves. En versiones anteriores de vSphere, el servidor de claves se llamaba servidor de administración de claves o KMS. Actualmente, el cifrado de máquinas virtuales de vSphere admite servidores de claves compatibles con KMIP 1.1.

Cómo almacena vSphere Trust Authority información de estado y configuración

vCenter Server es principalmente un servicio de acceso directo para obtener información sobre el estado y la configuración de vSphere Trust Authority. La mayor parte de la información de configuración y estado de vSphere Trust Authority se almacena en los hosts ESXi de la base de datos de ConfigStore. Parte de la información de estado también se almacena en la base de datos de vCenter Server.

Nota Debido a que la mayor parte de la información de configuración de vSphere Trust Authority se almacena en los hosts ESXi, el mecanismo de copia de seguridad basado en archivos de vCenter Server no incluye esta información en la copia de seguridad. Para garantizar que se hayan guardado los datos de configuración de la implementación de vSphere Trust Authority, consulte Realizar una copia de seguridad de la configuración de vSphere Trust Authority.

Cómo se integra vSphere Trust Authority con vCenter Server

Puede configurar instancias independientes de vCenter Server para administrar el clúster de Trust Authority y el clúster de confianza. Consulte Configurar vSphere Trust Authority.

En un clúster de confianza, vCenter Server administra las llamadas API de Trust Authority y las envía a los hosts ESXi. vCenter Server replica las llamadas API entre todos los hosts ESXi del clúster de confianza.

Después de configurar vSphere Trust Authority inicialmente, puede agregar o quitar hosts ESXi en un clúster de Trust Authority o un clúster de confianza. Consulte Agregar y eliminar hosts de vSphere Trust Authority.

Flujos de procesos de vSphere Trust Authority

Es esencial comprender los flujos de proceso de vSphere Trust Authority para saber cómo configurar y administrar la infraestructura de confianza.

Cómo configurar vSphere Trust Authority

vSphere Trust Authority no está activado de forma predeterminada. Debe configurar manualmente vSphere Trust Authority en el entorno. Consulte Configurar vSphere Trust Authority.

Cuando se configura vSphere Trust Authority, se deben especificar las versiones del software ESXi que acepta el servicio de atestación, así como los módulos de plataforma de confianza (Trusted Platform Modules, TPM) en los que se puede confiar.

TPM y atestación en vSphere Trust Authority

En esta guía, se utilizan las siguientes definiciones al describir los TPM y la atestación.

Tabla 9-2. Glosario de TPM y atestación

Término	Definición
Clave de aprobación (EK)	Un TPM se genera con un par de claves pública/privada de RSA integradas en el hardware, lo que se denomina clave de aprobación (Endorsement Key, EK). La EK es única para un TPM en particular.
Clave pública EK	La parte pública del par de claves EK.
Clave privada de EK	La parte privada del par de claves EK.
Certificado de EK	La clave pública EK envuelta con una firma. El certificado de EK lo crea el fabricante del TPM que utiliza su clave privada de la entidad de certificación para firmar la clave pública EK. No todos los TPM contienen un certificado de EK. En este caso, la clave pública EK no está firmada.
Atestación de TPM	La capacidad del servicio de atestación para comprobar el software que se ejecuta en un host remoto. La atestación de TPM se realiza a través de mediciones criptográficas que realiza el TPM mientras el host remoto se inicia y se retransmite al servicio de atestación cuando se solicita. El servicio de atestación establece una relación de confianza en el TPM a través de la clave pública EK o el certificado de EK.

Configurar la confianza del TPM en los hosts de confianza

Un host ESXi de confianza debe contener un TPM. Un TPM se genera con un par de claves pública/privada integradas en el hardware, lo que se denomina clave de aprobación (Endorsement Key, EK). Aunque TPM 2.0 permite muchos pares de clave/certificado, el más común es un par de claves RSA-2048. Cuando una CA firma una clave pública EK de TPM, el resultado es el certificado de EK. Por lo general, el fabricante del TPM genera previamente al menos una EK, firma la clave pública con una entidad de certificación e inserta el certificado firmado en la memoria no volátil del TPM.

Puede configurar el servicio de atestación para que confíe en los TPM de la siguiente manera:

- Confiar en todos los certificados de CA con los que el fabricante firmó el TPM (la clave pública EK). La configuración predeterminada del servicio de atestación es confiar en los certificados de CA. En este enfoque, el mismo certificado de CA abarca varios hosts ESXi y, por lo tanto, reduce la sobrecarga administrativa.
- Confiar en el certificado de CA de TPM y la clave pública EK del host ESXi. La clave puede ser el certificado de EK o la clave pública EK. Aunque este enfoque proporciona más seguridad, requiere que vuelva a configurar la información sobre cada host de confianza.
- Algunos TPM no contienen un certificado de EK. En este caso, se confía en la clave pública EK.

La decisión de confiar en todos los certificados de CA del TPM es una operación adecuada. Solo se configuran certificados nuevos cuando se agrega una nueva clase de hardware al centro de datos. Al confiar en los certificados de EK individuales, puede limitar el acceso a hosts ESXi específicos.

También puede decidir no confiar en certificados de CA del TPM. A pesar de que es una situación poco común, puede utilizar esta configuración cuando una CA no firma una EK. Actualmente, esta funcionalidad no está totalmente implementada.

Nota Algunos TPM no incluyen certificados de EK. Si desea confiar en hosts ESXi individuales, el TPM debe incluir un certificado de EK.

Cómo atesta vSphere Trust Authority los TPM

Para comenzar el proceso de atestación, el host ESXi de confianza en el clúster de confianza envía la clave pública EK y el certificado de EK preconfigurados al servicio de atestación en el clúster de Trust Authority. Cuando el servicio de atestación recibe la solicitud, busca la EK en su configuración, que puede ser la clave pública EK o el certificado de EK, o ambos, según la configuración. Si no hay casos válidos, el servicio de atestación rechaza la solicitud de atestación.

La EK no se utiliza directamente para la firma, por lo que se negocia una clave de atestación (AK o AIK). El protocolo de negociación garantiza que una AK recién creada se enlace a la EK comprobada anteriormente, lo que impide una situación de "man-in-the-middle" o una suplantación. Una vez que se negocia una AK, se vuelve a utilizar en solicitudes de atestación futuras, en lugar de generar una nueva cada vez.

El host ESXi de confianza lee los valores de oferta y PCR del TPM. La oferta está firmada por la AK. El host ESXi de confianza también lee el registro de eventos de TCG, que incluye todos los eventos que dieron como resultado el estado actual del PCR. Esta información del TPM se envía al servicio de atestación para su validación. El servicio de atestación verifica los valores de PCR mediante el registro de eventos.

Cómo funcionan los proveedores de claves con los servidores de claves

El servicio de proveedor de claves utiliza el concepto de proveedor de claves de confianza para ocultar las características del servidor de claves del resto del software del centro de datos. Cada proveedor de claves de confianza tiene una sola clave de cifrado principal configurada y hace referencia a uno o varios servidores de claves. La clave de cifrado principal está presente en los servidores de claves. Como parte de la configuración de vSphere Trust Authority, debe proporcionar la clave principal como una actividad independiente y activarla. El servicio de proveedor de claves puede tener varios proveedores de claves de confianza configurados. Cada proveedor de claves de confianza utiliza una clave principal diferente, pero puede hacer referencia al mismo servidor de claves de respaldo.

Cuando se agrega un nuevo proveedor de claves de confianza, el administrador de Trust Authority debe especificar el servidor de claves y un identificador de clave existente en ese servidor de claves.

En la siguiente figura, se muestra la relación entre el servicio de proveedor de claves y los servidores de claves.

Figura 9-3. Proveedor de claves y servidor de claves

Host ESXi en clúster de confianza
Máquina virtual
Cifrar datos con key-provider-2
Host ESXi en clúster de Trust Authority
key-provider-1
keyID = 1111-1111-1111
key-provider-2
keyID = 2222-2222-2222
key-provider-3
keyID = 3333-3333-3333
KMS 1
KMS 2

Después de configurar un proveedor de claves de confianza para un clúster de confianza, el servicio de proveedor de claves puede aceptar solicitudes para ejecutar operaciones criptográficas en ese proveedor de claves de confianza. Por ejemplo, en esta figura, se configuran tres proveedores de claves de confianza, dos para KMS-1 y otro para KMS-2. El host de confianza solicita una operación de cifrado para key-provider-2. El host de confianza solicita una clave de cifrado que se generará y devolverá, y utiliza esta clave de cifrado para realizar operaciones de cifrado.

El servicio de proveedor de claves utiliza la clave principal a la que hace referencia el key-provider-2 para cifrar los datos en texto sin formato especificados y devolver el texto cifrado correspondiente. Más adelante, el host de confianza puede proporcionar el mismo texto cifrado a una operación de descifrado y recuperar el texto sin formato original.

Autenticación y autorización de vSphere Trust Authority

Las operaciones administrativas de vSphere Trust Authority requieren un usuario que sea miembro del grupo de TrustedAdmins. No es suficiente tener solo privilegios de administrador de Trust Authority para realizar todas las operaciones administrativas que implican a los hosts ESXi. Para obtener más información, consulte Requisitos previos y privilegios necesarios para vSphere Trust Authority.

Agregar un host de confianza a un clúster de confianza

Los pasos para agregar hosts ESXi inicialmente al clúster de confianza se describen en Configurar vSphere Trust Authority.

Más adelante, si desea agregar hosts ESXi al clúster de confianza, el flujo de trabajo es diferente. Consulte Agregar y eliminar hosts de vSphere Trust Authority.

Cuando se agregan inicialmente hosts ESXi al clúster de confianza, se debe recopilar la siguiente información:

- Certificado de TPM para cada tipo de hardware en el clúster
- Imagen de ESXi de cada versión de ESXi en el clúster
- Información principal de vCenter Server

Si más tarde agregan hosts ESXi a un clúster de confianza, es posible que necesite recopilar información adicional. Es decir, si los hosts ESXi nuevos difieren en el hardware o la versión de ESXi de los hosts originales, debe recopilar la información del nuevo host ESXi e importarla en el clúster de Trust Authority. Solo debe recopilar la información principal de vCenter Server una vez por sistema vCenter Server.

Topología de vSphere Trust Authority

vSphere Trust Authority requiere sistemas vCenter Server independientes para el clúster de Trust Authority y el clúster de confianza.

El clúster de Trust Authority se configura y administra en una instancia de vCenter Server independiente y aislada. La instancia de vCenter Server del clúster de Trust Authority no puede ser también la instancia de vCenter Server del clúster de confianza. El clúster de confianza debe tener su propia instancia de vCenter Server independiente. Una única instancia de vCenter Server puede administrar varios clústeres de confianza. Varios sistemas vCenter Server para los clústeres de confianza pueden participar en Enhanced Linked Mode. Las instancias de vCenter Server para el clúster de Trust Authority no pueden participar en Enhanced Linked Mode con otros sistemas vCenter Server del clúster de Trust Authority o sistemas vCenter Server del clúster de confianza.

El administrador de Trust Authority administra el clúster de Trust Authority y sus instancias de vCenter Server asociadas de forma independiente de otras instancias de vCenter Server, ya que este enfoque proporciona el mejor aislamiento de seguridad.

El administrador de Trust Authority documenta o publica los nombres de host y certificados SSL que los administradores de clústeres de confianza utilizan para configurar los clústeres. El administrador de Trust Authority también aprovisiona proveedores de claves de confianza para la organización y sus departamentos, o incluso administradores individuales.

No se pueden implementar servicios de vSphere Trust Authority directamente en el clúster de confianza administrado por la instancia de vCenter Server de carga de trabajo, ya que el administrador de carga de trabajo tiene acceso de alto privilegio a los hosts ESXi. Este tipo de implementación no logra la separación necesaria de funciones que se requiere para cumplir los objetivos de seguridad de vSphere Trust Authority.

Requisitos previos y privilegios necesarios para vSphere Trust Authority

Debe tener en cuenta los requisitos de hardware y software al configurar vSphere Trust Authority. Debe establecer privilegios y funciones de cifrado para utilizar el cifrado. El usuario que realiza tareas de vSphere Trust Authority debe contar con los privilegios correspondientes.

Requisitos de vSphere Trust Authority

Para utilizar vSphere Trust Authority, el entorno de vSphere debe cumplir con estos requisitos:

- Requisitos de hardware del host de confianza ESXi:
  - TPM 2.0
  - Debe estar habilitado el arranque seguro
  - Firmware EFI.
- Requisitos de los componentes:
  - vCenter Server 7.0 o versiones posteriores
  - Un sistema de vCenter Server dedicado para el clúster de vSphere Trust Authority y los hosts ESXi
  - Un sistema de vCenter Server independiente para el clúster de confianza y los hosts ESXi de confianza
  - Un servidor de claves (llamado servidor de administración de claves, o KMS, en versiones anteriores de vSphere)
- Requisitos de la máquina virtual:
  - Firmware EFI.
  - Arranque seguro habilitado

Nota Antes de comenzar a configurar vSphere Trust Authority, asegúrese de haber configurado los sistemas de vCenter Server para el clúster de Trust Authority y el clúster de confianza, y de haber agregado hosts ESXi a cada clúster.

vSphere Trust Authority y privilegios de criptografía

vSphere Trust Authority no introduce ningún privilegio de cifrado nuevo. A vSphere Trust Authority se aplican los mismos privilegios de cifrado descritos en Usar las funciones y los privilegios de cifrado.

vSphere Trust Authority y el modo de cifrado de host

vSphere Trust Authority no introduce ningún nuevo requisito para habilitar el modo de cifrado de host en los hosts ESXi de confianza. Consulte Requisitos previos y privilegios necesarios para tareas de cifrado de máquinas virtuales para obtener más información sobre el modo de cifrado del host.

Usar las funciones de vSphere Trust Authority y el grupo TrustedAdmins

Para que vSphere Trust Authority funcione, se requiere un usuario que sea miembro del grupo TrustedAdmins. Este usuario se denomina administrador de Trust Authority. Los administradores de vSphere deben agregarse al grupo TrustedAdmins o agregar otros usuarios al grupo para obtener la función Administrador de infraestructura de confianza. La función Administrador de infraestructura de confianza es necesaria para la autorización de vCenter Server. El grupo TrustedAdmins es necesario para la autenticación en los hosts ESXi que forman parte de la infraestructura de confianza. Los usuarios con el privilegio **Operaciones criptográficas .Registrar host** en ESXi hosts pueden administrar el clúster de confianza. Los permisos vCenter Server no se propagan a los hosts de Trust Authority, solo a los hosts de confianza. Solo los miembros del grupo TrustedAdmins reciben privilegios en los hosts de Trust Authority. La membresía al grupo se verifica en el propio host ESXi.

Nota A los administradores de vSphere y miembros del grupo de administradores se les asigna la función Administrador de infraestructura de confianza, pero esta función en sí no permite que un usuario realice operaciones de vSphere Trust Authority. También se requiere ser miembro del grupo TrustedAdmins.

Una vez que vSphere Trust Authority está habilitado, los administradores de Trust Authority pueden asignar proveedores de claves de confianza a los hosts de confianza. Estos hosts de confianza pueden utilizar los proveedores de claves de confianza para realizar tareas de cifrado.

Además de la función Administrador de infraestructura de confianza, vSphere Trust Authority proporciona la función Sin administrador de infraestructura de confianza, que contiene todos los privilegios en vCenter Server, excepto los que llaman a las API de vSphere Trust Authority.

Los grupos, las funciones y los usuarios de vSphere Trust Authority funcionan de la siguiente manera:

- En el primer arranque, vSphere otorga al grupo TrustedAdmins la función Administrador de infraestructura de confianza, que tiene permisos globales.
- La función Administrador de infraestructuras de confianza es una función del sistema que tiene los privilegios necesarios para llamar a las API de vSphere Trust Authority (`TrustedAdmin.*`) y los privilegios del sistema **System.Read**, **System.View** y **System.Anonymous** para ver los objetos del inventario.
- La función Sin administrador de infraestructura de confianza es una función del sistema que contiene todos los privilegios en vCenter Server, excepto aquellos para llamar a las API de vSphere Trust Authority. Al agregar nuevos privilegios a vCenter Server, también se agregan a la función Sin administrador de infraestructura de confianza. (La función Sin administrador de infraestructura de confianza es similar a la función Sin administrador de criptografía).
- Los privilegios de vSphere Trust Authority (API de `TrustedAdmin.*`) no se incluyen en la función Sin administrador de criptografía, lo cual impide que los usuarios con esta función configuren una infraestructura de confianza o realicen operaciones criptográficas.

Los casos de uso para estos usuarios, grupos y funciones se muestran en la siguiente tabla.

Tabla 9-3. Usuarios, grupos y funciones de vSphere Trust Authority

Usuario, grupo o función	Puede llamar a la API de vCenter Server de vSphere Trust Authority (incluye llamadas a la API de ESXi de vSphere Trust Authority)	Puede llamar a la API de vCenter Server de vSphere Trust Authority (no incluye llamadas a la API de ESXi de vSphere Trust Authority)	Puede realizar operaciones de host en un clúster que no está relacionado con vSphere Trust Authority	Comentario
Usuario en el grupo Administrators@*system.domain* y en el grupo TrustedAdmins@*system.domain*	Sí	Sí	Sí	No corresponde
Usuario solo en el grupo TrustedAdmins@*system.domain*	Sí	Sí	No	Este tipo de usuario no puede realizar operaciones normales de administración de clústeres.
Usuario solo en el grupo Administrators@*system.domain*	Sí	No	Sí	No corresponde
Usuario con la función Administrador de infraestructura de confianza, pero no en el grupo TrustedAdmins@*system.domain*	Sí	No	No	El host ESXi comprueba que el usuario pertenece al grupo para conceder permisos.
Usuario solo con la función Sin administrador de infraestructura de confianza	No	No	Sí	Este tipo de usuario es similar a un administrador que no puede realizar operaciones de vSphere Trust Authority.

Prácticas recomendadas, advertencias e interoperabilidad de vSphere Trust Authority

La arquitectura de vSphere Trust Authority produce algunas recomendaciones adicionales. Tenga en cuenta las limitaciones de interoperabilidad al planear su estrategia de vSphere Trust Authority.

Interoperabilidad de la infraestructura de confianza

Para versiones de ESXi, el servicio de atestación es compatible con versiones anteriores y posteriores. Por ejemplo, puede tener un clúster de hosts ESXi que ejecutan ESXi 7.0 en el clúster de vSphere Trust Authority y actualizar o aplicar revisiones a hosts ESXi del clúster de confianza a una versión más reciente de ESXi. De forma similar, puede actualizar o aplicar revisiones a los hosts ESXi del clúster de Trust Authority y, a la vez, mantener los hosts ESXi en el clúster de confianza en la versión actual.

No puede tener una función de clúster como clúster de Trust Authority y como clúster de confianza. Esta configuración no es compatible.

Limitación de la configuración del clúster de confianza

Solo puede configurar un clúster de Trust Authority por carga de trabajo de vCenter Server. No se puede configurar un clúster de confianza para hacer referencia a varios clústeres de Trust Authority.

Características de vSphere compatibles en vSphere Trust Authority

vSphere Trust Authority admite lo siguiente:

- vCenter High Availability (vCenter HA)
- VMware vSphere High Availability
- DRS
- DPM
- SRM, con los siguientes conocimientos:
  - Se admite SRM con replicación basada en matrices si la misma configuración de servicios de vSphere Trust Authority está disponible en el lado de recuperación.
  - SPPG
- VADP
  - La compatibilidad es igual que con el cifrado estándar. Se admiten los modos de agregado en caliente y NFC, pero no el modo SAN. Las copias de seguridad se descifran. Los socios de VADP tienen la opción de recuperar la máquina virtual de copia de seguridad con la misma clave de cifrado que la máquina virtual original.
- vSAN
  - El cifrado de máquinas virtuales es totalmente compatible con vSAN.
- OVF
  - Las máquinas virtuales cifradas no se pueden exportar a OVF. Sin embargo, las máquinas virtuales se pueden cifrar mientras se importan de un OVF.
- vVol

Características de vSphere no compatibles en vSphere Trust Authority

Actualmente, vSphere Trust Authority no es compatible con lo siguiente:

- Cifrado de datos en reposo de vSAN
- Cifrado de disco de primera clase (First Class Disk, FCD)
- vSphere Replication
- Perfiles de host de vSphere

Ciclo de vida de vSphere Trust Authority

Los servicios de vSphere Trust Authority se empaquetan y se instalan como parte de la imagen base de ESXi.

Iniciar y detener servicios de vSphere Trust Authority

En vSphere Client, puede iniciar, detener y reiniciar servicios de vSphere Trust Authority que están en ejecución en un host ESXi. Puede reiniciar servicios después de cambiar una configuración o si sospecha que hay problemas funcionales o de rendimiento. Para reiniciar el servicio en un host ESXi de confianza, debe iniciar sesión en el host. Consulte Iniciar, detener y reiniciar los servicios de vSphere Trust Authority.

Actualizar y aplicar revisiones en vSphere Trust Authority

Cada vez que actualiza o aplica una revisión a un host ESXi de confianza, debe actualizar el clúster de vSphere Trust Authority con la información de la nueva versión de ESXi. Para hacerlo, puede actualizar o aplicar la revisión a un host ESXi de prueba, exportar la información de la imagen base de ESXi, importar el archivo de imagen en el clúster de Trust Authority y, a continuación, actualizar o aplicar la revisión a los hosts ESXi de confianza.

Prácticas recomendadas para actualizaciones de vSphere Trust Authority

La práctica recomendada para actualizar una infraestructura de vSphere Trust Authority es actualizar primero el vCenter Server y los hosts de Trust Authority. De esta forma, obtendrá el máximo beneficio de las funciones más recientes de vSphere Trust Authority. Sin embargo, puede realizar actualizaciones independientes del vCenter Server y los hosts ESXi para responder a motivos empresariales específicos.

En general, siga este orden para actualizar la infraestructura de vSphere Trust Authority:

1. Actualice el vCenter Server de clústeres de Trust Authority.
2. Actualice los hosts de Trust Authority.
3. Actualice el vCenter Server de clústeres de confianza.
4. Actualice los hosts de confianza.

Para garantizar que no haya complicaciones en el proceso, actualice los hosts de Trust Authority y los hosts de confianza de forma gradual, uno a uno.

Actualizar vSphere Trust Authority con hosts de confianza de Quick Booted ESXi

Quick Boot es una opción que se puede utilizar con clústeres que se administran con imágenes de vSphere Lifecycle Manager y líneas base de vSphere Lifecycle Manager. Al usar Quick Boot, se optimizan las operaciones de actualización y aplicación de revisiones en los hosts ESXi.

Cuando se actualiza un host ESXi mediante la optimización de Quick Boot; la atestación de host sigue informando de la versión de ESXi arrancada anteriormente en la raíz de la medición de confianza.

Por lo tanto, cuando actualice un host ESXi de confianza que esté habilitado para Quick Boot y que forme parte de una implementación de vSphere Trust Authority, preste atención a lo siguiente:

1 No elimine del servicio de atestación la versión de la imagen base de ESXi en la que inicialmente confiaba hasta que todos los hosts ESXi hayan completado un reinicio completo después de la actualización. (Si necesita reiniciar el host, deshabilite Quick Boot).

2 Si utilizó Quick Boot para varias actualizaciones y desea eliminar una versión de ESXi intermedia que ya no sea de confianza, utilice la API de `base-images` para confirmar la versión de ESXi que atestó por última vez.

3 Al exportar la imagen base de ESXi de un host ESXi habilitado para Quick Boot, aparece un mensaje que indica que el host se actualizó mediante Quick Boot. El archivo resultante contiene los metadatos más recientes de la imagen base de ESXi.

Si actualiza los hosts de un clúster normal mediante Quick Boot, y posteriormente agrega ese clúster a vSphere Trust Authority, los hosts no atestarán hasta que los reinicie. El error de atestación se produce debido a que el archivo de imagen base de ESXi exportado de los hosts contiene solo los metadatos más recientes, mientras que la atestación del host se basa en los metadatos del último arranque completo. Por lo tanto, si el clúster no forma parte de vSphere Trust Authority y los metadatos de la imagen base ESXi no se importan a vSphere Trust Authority para el arranque completo, se produce un error en la atestación.

Para obtener la imagen base, puede utilizar los siguientes comandos de PowerCLI.

```
$vTA = Get-TrustAuthorityCluster -name trustedCluster
$bm = Get-TrustAuthorityVMHostBaseImage $vTA
$bm | select *
```

Solucionar problemas de actualización de vSphere Trust Authority

Si un host de Trust Authority no se actualiza correctamente, siga estos pasos.

1 Elimine el host de Trust Authority del clúster de confianza.

2 Revierta a la versión anterior de ESXi.

3 Vuelva a agregar el host de Trust Authority al clúster, como se describe en el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/77234.

4 Compruebe que la configuración del host de Trust Authority sea coherente con los demás hosts de Trust Authority en el clúster de Trust Authority. Consulte Comprobar el estado del clúster de confianza.

Cuando se actualiza a una nueva versión de ESXi en un host de confianza, se produce un error en la atestación hasta que se actualiza el clúster de Trust Authority con la información de la nueva imagen base ESXi. Este comportamiento es el esperado. Ya no es posible cifrar máquinas virtuales ni utilizar máquinas virtuales existentes que se hayan cifrado antes de la actualización hasta que se solucione el problema. Los mensajes de error de atestación aparecen en el panel **Tareas recientes** de vSphere Client y en los archivos `attestd.log`, `kmxa.log` y `vpxd.log`.

Para corregir el problema, siga estos pasos.

1 Ejecute el cmdlet `Export-VMHostImageDb` para volver a exportar las imágenes base de ESXi. Consulte el paso 5 de Recopilar información sobre hosts ESXi e instancias de vCenter Server que serán de confianza.

2 Ejecute el cmdlet `New-TrustAuthorityVMHostBaseImage` para volver a importar la nueva imagen base al vCenter Server del clúster de Trust Authority. Consulte el paso 8 de Importar la información del host de confianza en el clúster de Trust Authority.

3 Si ya no es necesario que ateste las versiones anteriores de ESXi (se actualizaron todos los hosts de confianza), ejecute el cmdlet `Remove-TrustAuthorityVMHostBaseImage` para eliminar las versiones. Por ejemplo:

```
$vTA = Get-TrustAuthorityCluster 'vTA Cluster'
$baseImages = Get-TrustAuthorityVMHostBaseImage -TrustAuthorityCluster $vTA
Remove-TrustAuthorityVMHostBaseImage -VMHostBaseImage $baseImages
```

Realizar una copia de seguridad de la configuración de vSphere Trust Authority

Debido a que la mayor parte de la información de configuración de vSphere Trust Authority se almacena en los hosts ESXi, la copia de seguridad de vCenter Server no incluye esta información de vSphere Trust Authority. Consulte Realizar una copia de seguridad de la configuración de vSphere Trust Authority.

Configurar vSphere Trust Authority

vSphere Trust Authority no está habilitado de forma predeterminada. Para poder empezar a utilizar vSphere Trust Authority, debe configurar el entorno.

Hay que habilitar los servicios de vSphere Trust Authority en un clúster de vCenter Server dedicado (lo que se conoce como clúster de vSphere Trust Authority). El clúster de Trust Authority actúa como una plataforma de administración centralizada y segura. Luego, hay que habilitar un clúster de vCenter Server de carga de trabajo como clúster de confianza. El clúster de confianza contiene los hosts ESXi de confianza.

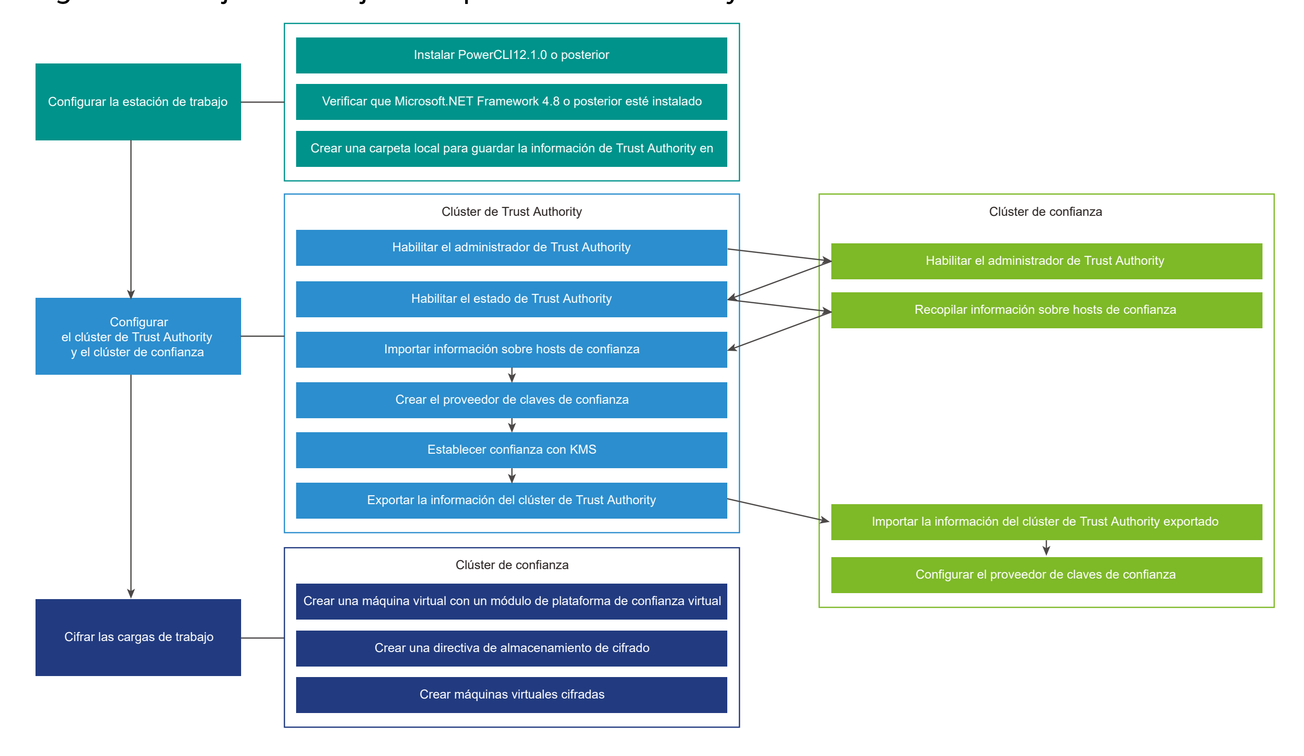
El clúster de Trust Authority certifica los hosts ESXi del clúster de confianza de forma remota. El clúster de Trust Authority publica claves de cifrado únicamente para los hosts ESXi certificados en el clúster de confianza para cifrar máquinas virtuales y discos virtuales mediante proveedores de claves de confianza.

Antes de empezar a configurar vSphere Trust Authority, consulte Requisitos previos y privilegios necesarios para vSphere Trust Authority para obtener información sobre la configuración necesaria de los sistemas vCenter Server y los hosts ESXi.

Se pueden administrar diferentes aspectos de vSphere Trust Authority de las siguientes maneras.

- Configure los servicios y las conexiones de confianza de vSphere Trust Authorityusando cmdlets de PowerCLI o las API de vSphere. Consulte *Referencia de cmdlets de VMware PowerCLI* y *Guía de programación de vSphere Automation SDK*.
- Administre la configuración de proveedores de claves de confianza mediante los cmdlets de PowerCLI o en vSphere Client.
- Realice flujos de trabajo de cifrado, como en versiones anteriores de vSphere, usando API y vSphere Client.

Figura 9-4. Flujo de trabajo de vSphere Trust Authority



Para configurar y administrar vSphere Trust Authority, utilice VMware PowerCLI, aunque algunas funcionalidades estén disponibles en vSphere Client.

Cuando vSphere Trust Authority se configura, hay que completar las tareas de configuración tanto en el clúster de Trust Authority como en el clúster de confianza. Algunas de estas tareas deben realizarse en orden. Utilice la secuencia de tareas que se describe en esta guía.

Nota Cuando se agregan más hosts ESXi al clúster de confianza después de completar la configuración inicial de vSphere Trust Authority, es posible que sea necesario exportar e importar de nuevo la información de los hosts de confianza. Es decir, si los hosts ESXi nuevos difieren de los hosts originales, deberá recopilar la información de esos hosts ESXinuevos e importarla al clúster de Trust Authority. Consulte Agregar y eliminar hosts de vSphere Trust Authority.

Qué leer a continuación

Procedimiento

1 Configurar Workstation para configurar vSphere Trust Authority

   Para configurar una implementación de vSphere Trust Authority, primero debe preparar una estación de trabajo con el software y la configuración necesarios.

2 Habilitar el administrador de Trust Authority

   Para habilitar vSphere Trust Authority, debe agregar un usuario al grupo TrustedAdmins de vSphere. Este usuario se convierte en el administrador de Trust Authority. El administrador de Trust Authority se utiliza en la mayoría de las tareas de configuración de vSphere Trust Authority.

3 Habilitar el estado de Trust Authority

   Al convertir un clúster de vCenter Server en un clúster de vSphere Trust Authority (lo que también se denomina habilitar el estado de Trust Authority), se inician los servicios de Trust Authority requeridos en los hosts ESXi del clúster.

4 Recopilar información sobre hosts ESXi e instancias de vCenter Server que serán de confianza

   Para establecer la confianza, el clúster de vSphere Trust Authority requiere información acerca de los hosts ESXi y la instancia de vCenter Server del clúster de confianza. Esta información se exporta como archivos para importarlos al clúster de Trust Authority. Debe asegurarse de mantener la confidencialidad de estos archivos y de transportarlos de forma segura.

5 Importar la información del host de confianza en el clúster de Trust Authority

   Importe el host ESXi exportado y la información de vCenter Server en el clúster de vSphere Trust Authority, para que el clúster de Trust Authority sepa los hosts que puede atestar.

6 Crear el proveedor de claves en el clúster de Trust Authority

Para que el servicio de proveedor de claves se conecte a un proveedor de claves, primero debe crear un proveedor de claves de confianza y, a continuación, establecer una configuración de confianza entre el clúster de vSphere Trust Authority y el servidor de claves (Key Management Server, KMS). Para la mayoría de los servidores de claves que cumplen con KMIP, esta configuración implica el establecimiento de certificados de cliente y servidor.

7 Exportar la información del clúster de Trust Authority

Respecto al clúster de confianza que se va a conectar al clúster de vSphere Trust Authority, debe exportar la información del servicio del clúster de Trust Authority como un archivo y, a continuación, importar dicho archivo al clúster de confianza. Debe asegurarse de mantener la confidencialidad de este archivo y de transportarlo de forma segura.

8 Importar la información del clúster de Trust Authority en los hosts de confianza

Después de importar la información del clúster de vSphere Trust Authority al clúster de confianza, los hosts de confianza inician el proceso de atestación con el clúster de Trust Authority.

9 Configurar el proveedor de claves de confianza para hosts de confianza mediante vSphere Client

Puede configurar el proveedor de claves de confianza mediante vSphere Client.

10 Configurar el proveedor de claves de confianza para hosts de confianza mediante la línea de comandos

Puede configurar proveedores de claves de confianza mediante la línea de comandos. Puede configurar el proveedor de claves de confianza predeterminado de vCenter Server o en el nivel del clúster o de carpeta de clúster en la jerarquía de objetos de vCenter.

Configurar Workstation para configurar vSphere Trust Authority

Para configurar una implementación de vSphere Trust Authority, primero debe preparar una estación de trabajo con el software y la configuración necesarios.

Realice los siguientes pasos en una estación de trabajo que tenga acceso a su entorno de vSphere Trust Authority.

Procedimiento

1 Instale PowerCLI 12.1.0 o posterior. Consulte la *Guía del usuario de PowerCLI*.

2 Compruebe que se haya instalado Microsoft .NET Framework 4.8 o una versión posterior.

3 Cree una carpeta local en la que desee guardar la información de Trust Authority que se va a exportar como archivos.

Pasos siguientes

Continúe con Habilitar el administrador de Trust Authority.

Habilitar el administrador de Trust Authority

Para habilitar vSphere Trust Authority, debe agregar un usuario al grupo TrustedAdmins de vSphere. Este usuario se convierte en el administrador de Trust Authority. El administrador de Trust Authority se utiliza en la mayoría de las tareas de configuración de vSphere Trust Authority.

Utilice un usuario aparte del administrador de vCenter Server como administrador de Trust Authority. Tener un usuario aparte mejora la seguridad del entorno. Debe habilitar un administrador de Trust Authority tanto para el clúster de Trust Authority como para el clúster de confianza.

Requisitos previos

Cree un usuario, o bien identifique un usuario existente para que sea el administrador de Trust Authority.

Procedimiento

1. Conéctese a la instancia de vCenter Server del clúster de Trust Authority mediante vSphere Client.
2. Inicie sesión como administrador.
3. En el menú **Inicio**, seleccione **Administración**.
4. En **Single Sign-On**, haga clic en **Usuarios y grupos**.
5. Haga clic en **Grupos** y, a continuación, en el grupo **TrustedAdmins**.

   Si el grupo TrustedAdmins no aparece inicialmente, utilice el icono **Filtrar** para encontrarlo mediante un filtro, o desplácese por los grupos haciendo clic en la flecha derecha situada en la parte inferior del panel.
6. En el área **Miembros de grupo**, haga clic en **Agregar miembros**.

   Asegúrese de que el origen de identidad local está seleccionado (vsphere.local es el predeterminado, pero es posible que se seleccionara otro dominio durante la instalación) y busque el miembro (usuario) que desea agregar al grupo como administrador de Trust Authority.
7. Seleccione al miembro.
8. Haga clic en **Guardar**.
9. Repita los pasos 1 a 8 para la instancia de vCenter Server del clúster de confianza.

Pasos siguientes

Continúe con Habilitar el estado de Trust Authority.

Habilitar el estado de Trust Authority

Al convertir un clúster de vCenter Server en un clúster de vSphere Trust Authority (lo que también se denomina habilitar el estado de Trust Authority), se inician los servicios de Trust Authority requeridos en los hosts ESXi del clúster.

Requisitos previos

- Habilitar el administrador de Trust Authority.

Procedimiento

1 En una sesión de PowerCLI, ejecute el cmdlet `Connect-VIServer` para conectarse como usuario administrador de Trust Authority a la instancia de vCenter Server del clúster de Trust Authority.

```
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

2 Para comprobar el estado actual del clúster, ejecute el cmdlet `Get-TrustAuthorityCluster`.

Por ejemplo, este comando muestra el clúster, `vTA Cluster`, y que su estado es deshabilitado.

```
Get-TrustAuthorityCluster

Name                 State                Id
----                 -----                --
vTA Cluster          Disabled             TrustAuthorityCluster-domain-c8
```

El resultado muestra Deshabilitado o Habilitado en la columna Estado de cada clúster encontrado. Deshabilitado significa que los servicios de Trust Authority no se están ejecutando.

3 Para habilitar el clúster de Trust Authority, ejecute el cmdlet `Set-TrustAuthorityCluster`.

Por ejemplo, este comando habilita el clúster `vTA Cluster`.

```
Set-TrustAuthorityCluster -TrustAuthorityCluster 'vTA Cluster' -State Enabled
```

El sistema responde con un mensaje de confirmación.

```
Confirmation
Setting TrustAuthorityCluster 'vTA Cluster' with new State 'Enabled'. Do you want to
proceed?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
```

4 En la solicitud de confirmación, presione Intro. (El valor predeterminado es **Y**).

El resultado mostrará el estado del clúster. Por ejemplo, a continuación se muestra que el clúster `vTA Cluster` se habilitó:

```
Name                 State                Id
----                 -----                --
vTA Cluster          Enabled              TrustAuthorityCluster-domain-c8
```

Resultados

Se inician dos servicios en los hosts ESXi en el clúster de Trust Authority: el servicio de atestación y el servicio de proveedor de claves.

Ejemplo: Habilitar el estado de confianza en el clúster de Trust Authority

En este ejemplo, se muestra cómo usar PowerCLI para habilitar servicios en el clúster de Trust Authority. En la siguiente tabla, se muestran los componentes y los valores de ejemplo que se utilizan.

Tabla 9-4. Ejemplo de configuración de vSphere Trust Authority

Componente	Valor
vCenter Server para clúster de Trust Authority	192.168.210.22
Nombre del clúster de Trust Authority	Clúster de vTA
Administrador de Trust Authority	trustedadmin@vsphere.local

```
PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.210.22                 443   VSPHERE.LOCAL\trustedadmin

PS C:\Users\Administrator.CORP> Get-TrustAuthorityCluster

Name                 State                Id
----                 -----                --
vTA Cluster          Disabled             TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator.CORP> Set-TrustAuthorityCluster -TrustAuthorityCluster 'vTA
Cluster' -State Enabled

Confirmation
Setting TrustAuthorityCluster 'vTA Cluster' with new State 'Enabled'. Do you want to proceed?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): y

Name                 State                Id
----                 -----                --
vTA Cluster          Enabled              TrustAuthorityCluster-domain-c8
```

Pasos siguientes

Continúe con Recopilar información sobre hosts ESXi e instancias de vCenter Server que serán de confianza.

Recopilar información sobre hosts ESXi e instancias de vCenter Server que serán de confianza

Para establecer la confianza, el clúster de vSphere Trust Authority requiere información acerca de los hosts ESXi y la instancia de vCenter Server del clúster de confianza. Esta información se exporta como archivos para importarlos al clúster de Trust Authority. Debe asegurarse de mantener la confidencialidad de estos archivos y de transportarlos de forma segura.

Utilice cmdlets de PowerCLI de vSphere Trust Authority para exportar la siguiente información como archivos a partir de los hosts de ESXi en el clúster de confianza para que el clúster de Trust Authority sepa en qué software y hardware puede confiar.

- Versión de ESXi
- Fabricante del TPM (certificado de CA)
- (Opcional) TPM individual (certificado de EK)

Nota Almacene estos archivos exportados en una ubicación segura, en caso de que deba restaurar la configuración de vSphere Trust Authority.

Si tiene hosts del mismo tipo y proveedor y fabricados durante el mismo período de tiempo y ubicación, es posible que pueda confiar en todos los TPM; para ello, debe obtener el certificado de CA de solo uno de los TPM. Para confiar en un TPM individual, obtenga el certificado de EK de TPM.

También debe obtener la información principal de la instancia de vCenter Server del clúster de confianza. La información principal contiene el usuario de solución vpxd y su cadena de certificados. La información principal permite que la instancia de vCenter Server del clúster de confianza detecte los proveedores de claves de confianza disponibles configurados en el clúster de Trust Authority.

Para configurar inicialmente vSphere Trust Authority, debe recopilar la versión de ESXi y la información del TPM. También debe recopilar la versión de ESXi cada vez que implemente una nueva versión de ESXi, incluso cuando actualice o aplique una revisión.

La información principal de la instancia de vCenter Server solo se recopila una vez por sistema vCenter Server.

Requisitos previos

- Identifique las versiones de ESXi y los tipos de hardware de TPM que se encuentran en el clúster de confianza, y si desea confiar en todos los tipos de hardware de TPM, solo en algunos o en hosts individuales.

- En el equipo en el que ejecute los cmdlets de PowerCLI, cree una carpeta local en la que guardar la información que exporte como archivos.
- Habilitar el administrador de Trust Authority.
- Habilitar el estado de Trust Authority.

Procedimiento

1 En una sesión de PowerCLI, ejecute los siguientes comandos para desconectar cualquier conexión actual y conectarse como usuario raíz a uno de los hosts ESXi en el clúster de confianza.

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server host_ip_address -User root -Password 'password'
```

2 Ejecute el cmdlet `Get-VMHost` para confirmar el host ESXi.

```
Get-VMHost
```

Se mostrará la información del host.

3 Asigne `Get-VMHost` a una variable.

Por ejemplo:

```
$vmhost = Get-VMHost
```

4 Ejecute el cmdlet `Export-Tpm2CACertificate` para exportar el certificado de CA de un fabricante de TPM determinado.

a Asigne `Get-Tpm2EndorsementKey -VMHost $vmhost` a una variable.

Por ejemplo, este comando asigna `Get-Tpm2EndorsementKey -VMHost $vmhost` a la variable `$tpm2`.

```
$tpm2 = Get-Tpm2EndorsementKey -VMHost $vmhost
```

b Ejecute el cmdlet `Export-Tpm2CACertificate`.

Por ejemplo, este comando exporta el certificado de TPM al archivo `cacert.zip`. Antes de ejecutar este comando, asegúrese de que el directorio de destino existe.

```
Export-Tpm2CACertificate -Tpm2EndorsementKey $tpm2 -FilePath C:\vta\cacert.zip
```

Se creará el archivo.

c Repita el procedimiento para cada tipo de hardware de TPM en el clúster en el que desea confiar. Utilice un nombre de archivo diferente con cada tipo de hardware de TMP, así evitará sobrescribir un archivo previamente exportado.

5 Ejecute el cmdlet `Export-VMHostImageDb` para exportar la descripción del host ESXi del software (la imagen de ESXi).

Por ejemplo, este comando exporta la información al archivo `image.tgz`. Antes de ejecutar este comando, asegúrese de que el directorio de destino existe.

```
Export-VMHostImageDb -VMHost $vmhost -FilePath C:\vta\image.tgz
```

Nota El cmdlet `Export-VMHostImageDb` también funciona si prefiere iniciar sesión en la instancia de vCenter Server del clúster de confianza.

Se creará el archivo.

Repita los pasos para cada versión de ESXi en el clúster en el que desea confiar. Utilice un nombre de archivo diferente con cada versión, así evitará sobrescribir un archivo previamente exportado.

6 Exporte la información de entidad de seguridad de la instancia de vCenter Server del clúster de confianza.

a Desconéctese del host ESXi.

```
Disconnect-VIServer -server * -Confirm:$false
```

b Conéctese a la instancia de vCenter Server del clúster de confianza mediante el usuario administrador de Trust Authority. (También puede utilizar un usuario que tenga privilegios de **administrador**).

```
Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password
'password'
```

c Para exportar la información de entidad de seguridad de vCenter Server del clúster de confianza, ejecute el cmdlet `Export-TrustedPrincipal`.

Por ejemplo, este comando exporta la información al archivo `principal.json` . Antes de ejecutar este comando, asegúrese de que el directorio de destino existe.

```
Export-TrustedPrincipal -FilePath C:\vta\principal.json
```

Se creará el archivo.

7 (opcional) Si desea confiar en un host individual, debe exportar el certificado de clave pública EK de TPM.

Consulte Exportar e importar un certificado de clave de aprobación de TPM.

Resultados

Se crearán los siguientes archivos:

- Archivo de certificado de CA de TPM (extensión de archivo .zip)

- Archivo de imagen de ESXi (extensión de archivo .tgz)
- Archivo principal de vCenter Server (extensión de archivo .json)

Ejemplo: Recopilar información sobre hosts ESXi e instancias de vCenter Server que serán de confianza

En este ejemplo se muestra cómo usar PowerCLI para exportar la información del host ESXi y la entidad de seguridad de vCenter Server. En la siguiente tabla, se muestran los componentes y los valores de ejemplo que se utilizan.

Tabla 9-5. Ejemplo de configuración de vSphere Trust Authority

Componente	Valor
Host ESXi en un clúster de confianza	192.168.110.51
vCenter Server para clúster de confianza	192.168.110.22
Variable `$vmhost`	`Get-VMHost`
Variable `$tpm2`	`Get-Tpm2EndorsementKey -VMHost $vmhost`
Administrador de Trust Authority	trustedadmin@vsphere.local
Directorio local que contiene los archivos de salida	`C:\vta`

```
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.110.51 -User root -Password
'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.110.51                  443  root

PS C:\Users\Administrator.CORP> Get-VMHost

Name               ConnectionState PowerState NumCpu CpuUsageMhz CpuTotalMhz MemoryUsageGB
MemoryTotalGB Version
----               --------------- ---------- ------ ----------- ----------- -------------
------------- -------
192.168.110.51     Connected       PoweredOn       4         200        9576
1.614         7.999   7.0.0

PS C:\Users\Administrator.CORP> $vmhost = Get-VMHost
PS C:\Users\Administrator.CORP> $tpm2 = Get-Tpm2EndorsementKey -VMHost $vmhost
PS C:\> Export-Tpm2CACertificate -Tpm2EndorsementKey $tpm2 -FilePath C:\vta\cacert.zip

Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        10/8/2019   6:55 PM           1004 cacert.zip

PS C:\Users\Administrator.CORP> Export-VMHostImageDb -VMHost $vmhost -FilePath
C:\vta\image.tgz

Mode                LastWriteTime         Length Name
```

```
----                 -------------         ------ ----
-a----         10/8/2019  11:02 PM          2391 image.tgz

PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.110.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.110.22                  443  VSPHERE.LOCAL\trustedadmin

PS C:\Users\Administrator.CORP> Export-TrustedPrincipal -FilePath C:\vta\principal.json

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         10/8/2019  11:14 PM           1873 principal.json
```

Pasos siguientes

Continúe con Importar la información del host de confianza en el clúster de Trust Authority.

Exportar e importar un certificado de clave de aprobación de TPM

Puede exportar un certificado de clave de aprobación (Endorsement Key, EK) de TPM desde un host ESXi e importarlo al clúster de vSphere Trust Authority. Esto se hace cuando se quiere confiar en un host ESXi concreto en el clúster de confianza.

Para importar un certificado de EK de TPM al clúster de Trust Authority, hay que cambiar el tipo de atestación predeterminado del clúster de Trust Authority para que acepte certificados de EK. El tipo de atestación predeterminado acepta certificados de la entidad de certificación (Certificate Authority, CA) de TPM. Algunos TPM no incluyen certificados de EK. Si desea confiar en hosts ESXi individuales, el TPM debe incluir un certificado de EK.

Nota Almacene los archivos de certificado de EK en una ubicación segura, por si necesita restaurar la configuración de vSphere Trust Authority.

Requisitos previos

- Habilitar el administrador de Trust Authority.
- Habilitar el estado de Trust Authority.

Procedimiento

1 Asegúrese de que está conectado como administrador de Trust Authority a la instancia de vCenter Server del clúster de Trust Authority.

  Por ejemplo, puede introducir `$global:defaultviservers` para mostrar todos los servidores conectados.

2 (opcional) Si es necesario, puede ejecutar los siguientes comandos para asegurarse de que está conectado a la instancia de vCenter Server del clúster de Trust Authority.

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

3 Para cambiar el tipo de atestación del clúster de Trust Authority:

   a Ejecute el cmdlet `Get-TrustAuthorityCluster` para mostrar los clústeres que esta instancia de vCenter Server administra.

   ```
   Get-TrustAuthorityCluster
   ```

   Se mostrarán los clústeres.

   b Asigne la información de `Get-TrustAuthorityCluster` a una variable.

   Por ejemplo, este comando asigna el clúster con el nombre `vTA Cluster` a la variable `$vTA`.

   ```
   $vTA = Get-TrustAuthorityCluster 'vTA Cluster'
   ```

   c Asigne la información de `Get-TrustAuthorityTpm2AttestationSettings` a una variable.

   Por ejemplo, este comando asigna la información a la variable `$tpm2Settings`.

   ```
   $tpm2Settings = Get-TrustAuthorityTpm2AttestationSettings -TrustAuthorityCluster $vTA
   ```

d Ejecute el cmdlet `Set-TrustAuthorityTpm2AttestationSettings`, especificando `RequireEndorsementKey` o `RequireCertificateValidation`, o ambos.

Por ejemplo, este comando especifica `RequireEndorsementKey`.

```
Set-TrustAuthorityTpm2AttestationSettings -Tpm2AttestationSettings $tpm2Settings
-RequireEndorsementKey
```

El sistema responde con un mensaje de confirmación similar al siguiente.

```
Confirmation
Configure the Tpm2AttestationSettings 'TrustAuthorityTpm2AttestationSettings-domain-
c8' with the following parameters:
 RequireCertificateValidation: False
 RequireEndorsementKey: True
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
```

e En la solicitud de confirmación, presione Intro. (El valor predeterminado es **Y**).

La salida muestra un estado True de la configuración especificada. Por ejemplo, este estado muestra True en Solicitar clave de aprobación y False en Solicitar validación de certificado.

```
Name                                     RequireEndorsementKey
RequireCertificateValidation   Health
----                                     ---------------------
----------------------------   ------
TrustAuthorityTpm2AttestationSettings... True
False                          Ok
```

4 Para exportar el certificado EK de TPM:

a Desconéctese de la instancia de vCenter Server del clúster de Trust Authority.

```
Disconnect-VIServer -server * -Confirm:$false
```

b Ejecute el cmdlet `Connect-VIServer` para conectarse como usuario raíz a uno de los hosts ESXi en el clúster de confianza.

```
Connect-VIServer -server host_ip_address -User root -Password 'password'
```

c Ejecute el cmdlet `Get-VMHost` para confirmar el host ESXi.

```
Get-VMHost
```

Se mostrará la información del host.

d Asigne `Get-VMHost` a una variable.

Por ejemplo:

```
$vmhost = Get-VMHost
```

e Ejecute el cmdlet `Export-Tpm2EndorsementKey` para exportar el certificado de EK del host ESXi.

Por ejemplo, este comando exporta el certificado de EK al archivo `tpm2ek.json`.

```
Export-Tpm2EndorsementKey -VMHost $vmhost -FilePath C:\vta\tpm2ek.json
```

Se creará el archivo.

5 Para importar el EK de TPM:

a Desconéctese del host ESXi en el clúster de confianza.

```
Disconnect-VIServer -server * -Confirm:$false
```

b Conéctese a la instancia de vCenter Server del clúster de Trust Authority mediante el usuario administrador de Trust Authority.

```
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

c Ejecute el cmdlet `Get-TrustAuthorityCluster`.

```
Get-TrustAuthorityCluster
```

Se muestran los clústeres del clúster de Trust Authority.

d Asigne la información de `Get-TrustAuthorityCluster` '*clúster*' a una variable.

Por ejemplo, este comando asigna la información del clúster `vTA Cluster` a la variable `$vTA`.

```
$vTA = Get-TrustAuthorityCluster ‘vTA Cluster’
```

e Ejecute el cmdlet `New-TrustAuthorityTpm2EndorsementKey`.

Por ejemplo, este comando utiliza el archivo `tpm2ek.json` que se exportó anteriormente en el paso 4.

```
New-TrustAuthorityTpm2EndorsementKey -TrustAuthorityCluster $vTA -FilePath
C:\vta\tpm2ek.json
```

Se muestra información de la clave de aprobación importada.

Resultados

El tipo de atestación del clúster de Trust Authority se cambia para que se acepten certificados de EK. El certificado de EK se exporta desde el clúster de confianza y se importa al clúster de Trust Authority.

Ejemplo: Exportar e importar un certificado de EK de TPM

En este ejemplo, se muestra cómo utilizar PowerCLI para cambiar el tipo de atestación predeterminado del clúster de Trust Authority de forma que acepte certificados de EK, exportar el certificado EK de TPM del host ESXi en el clúster de confianza e importarlo al clúster de Trust Authority. En la siguiente tabla, se muestran los componentes y los valores de ejemplo que se utilizan.

Tabla 9-6. Ejemplo de configuración de vSphere Trust Authority

Componente	Valor
vCenter Server para clúster de Trust Authority	192.168.210.22
Variable `$vTA`	`Get-TrustAuthorityCluster 'vTA Cluster'`
Variable `$tpm2Settings`	`Get-TrustAuthorityTpm2AttestationSettings -TrustAuthorityCluster $vTA`
Variable `$vmhost`	`Get-VMHost`
Host ESXi en un clúster de confianza	192.168.110.51
Administrador de Trust Authority	trustedadmin@vsphere.local
Directorio local que contiene el archivo de salida	`C:\vta`

```
PS C:\Users\Administrator> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.210.22                 443   VSPHERE.LOCAL\TrustedAdmin

PS C:\Users\Administrator> Get-TrustAuthorityCluster

Name                 State              Id
----                 -----              --
vTA Cluster          Enabled            TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator> $vTA = Get-TrustAuthorityCluster 'vTA Cluster'

PS C:\Users\Administrator> $tpm2Settings = Get-TrustAuthorityTpm2AttestationSettings
-TrustAuthorityCluster $vTA

PS C:\Users\Administrator> Set-TrustAuthorityTpm2AttestationSettings -Tpm2AttestationSettings
$tpm2Settings -RequireEndorsementKey

Confirmation
```

```
Configure the Tpm2AttestationSettings 'TrustAuthorityTpm2AttestationSettings-domain-c8' with
the following parameters:
 RequireCertificateValidation: False
 RequireEndorsementKey: True
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): y

Name                                     RequireEndorsementKey
RequireCertificateValidation   Health
----                                     ---------------------
----------------------------   ------
TrustAuthorityTpm2AttestationSettings... True
False                          Ok

PS C:\Users\Administrator> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator> Connect-VIServer -server 192.168.110.51 -User root -Password
'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.110.51                 443   root

PS C:\Users\Administrator> Get-VMHost

Name                 ConnectionState PowerState NumCpu CpuUsageMhz CpuTotalMhz
MemoryUsageGB   MemoryTotalGB Version
----                 --------------- ---------- ------ ----------- -----------
-------------   ------------- -------
192.168.110.51       Connected       PoweredOn       4          55        9576
1.230           7.999   7.0.0

PS C:\Users\Administrator> $vmhost = Get-VMHost
PS C:\Users\Administrator> Export-Tpm2EndorsementKey -VMHost $vmhost -FilePath
C:\vta\tpm2ek.json

Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        12/3/2019  10:16 PM           2391 tpm2ek.json

PS C:\Users\Administrator> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.210.22                 443   VSPHERE.LOCAL\TrustedAdmin

PS C:\Users\Administrator> Get-TrustAuthorityCluster

Name                 State                Id
----                 -----                --
vTA Cluster          Enabled              TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator> $vTA = Get-TrustAuthorityCluster ‘vTA Cluster’
PS C:\Users\Administrator> New-TrustAuthorityTpm2EndorsementKey -TrustAuthorityCluster $vTA
-FilePath C:\vta\tpm2ek.json
```

```
TrustAuthorityClusterId                 Name                                    Health
-----------------------                 ----                                    ------
TrustAuthorityCluster-domain-c8         1a520e42-4db8-1cbb-6dd7-f493fd921ccb    Ok
```

Pasos siguientes

Continúe con Importar la información del host de confianza en el clúster de Trust Authority.

Importar la información del host de confianza en el clúster de Trust Authority

Importe el host ESXi exportado y la información de vCenter Server en el clúster de vSphere Trust Authority, para que el clúster de Trust Authority sepa los hosts que puede atestar.

Si sigue estas tareas en orden, aún está conectado a la instancia de vCenter Server del clúster de Trust Authority.

Requisitos previos

- Habilitar el administrador de Trust Authority.
- Habilitar el estado de Trust Authority.
- Recopilar información sobre hosts ESXi e instancias de vCenter Server que serán de confianza.

Procedimiento

1 Asegúrese de que está conectado como administrador de Trust Authority a la instancia de vCenter Server del clúster de Trust Authority.

   Por ejemplo, puede introducir `$global:defaultviservers` para mostrar todos los servidores conectados.

2 (opcional) Si es necesario, puede ejecutar los siguientes comandos para asegurarse de que está conectado a la instancia de vCenter Server del clúster de Trust Authority.

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

3 Para mostrar los clústeres administrados por esta instancia de vCenter Server, ejecute el cmdlet `Get-TrustAuthorityCluster`.

```
Get-TrustAuthorityCluster
```

   Se mostrarán los clústeres.

4 Asigne la información de `Get-TrustAuthorityCluster` '*clúster*' a una variable.

Por ejemplo, este comando asigna la información del clúster `vTA Cluster` a la variable `$vTA`.

```
$vTA = Get-TrustAuthorityCluster 'vTA Cluster'
```

5 Para importar la información de entidad de seguridad de la instancia de vCenter Server del clúster de confianza al clúster de Trust Authority, ejecute el cmdlet `New-TrustAuthorityPrincipal`.

Por ejemplo, el siguiente comando importa el archivo `principal.json` exportado previamente en Recopilar información sobre hosts ESXi e instancias de vCenter Server que serán de confianza.

```
New-TrustAuthorityPrincipal -TrustAuthorityCluster $vTA -FilePath C:\vta\principal.json
```

Se muestra la información de TrustAuthorityPrincipal.

6 Para comprobar la importación, ejecute el cmdlet `Get-TrustAuthorityPrincipal`.

Por ejemplo:

```
Get-TrustAuthorityPrincipal -TrustAuthorityCluster $vTA
```

Se muestra la información de TrustAuthorityPrincipal importada.

7 Para importar la información de certificado de CA del módulo de plataforma de confianza (Trusted Platform Module, TPM), ejecute el cmdlet `New-TrustAuthorityTpm2CACertificate`.

Por ejemplo, el siguiente comando importa la información del certificado de CA de TPM del archivo `cacert.zip` exportado previamente en Recopilar información sobre hosts ESXi e instancias de vCenter Server que serán de confianza.

```
New-TrustAuthorityTpm2CACertificate -TrustAuthorityCluster $vTA -FilePath
C:\vta\cacert.zip
```

Se muestra la información del certificado importado.

8 Para importar la información de la imagen base del host ESXi, ejecute el cmdlet `New-TrustAuthorityVMHostBaseImage`.

Por ejemplo, el siguiente comando importa la información de la imagen del archivo `image.tgz` exportado previamente en Recopilar información sobre hosts ESXi e instancias de vCenter Server que serán de confianza.

```
New-TrustAuthorityVMHostBaseImage -TrustAuthorityCluster $vTA -FilePath C:\vta\image.tgz
```

Se mostrará la información de la imagen importada.

Resultados

El clúster de Trust Authority sabe qué hosts ESXi puede atestar de forma remota y, por lo tanto, en qué hosts puede confiar.

Ejemplo: Importar la información del host de confianza en el clúster de Trust Authority

En este ejemplo se muestra cómo usar PowerCLI para importar la información de la entidad de seguridad de vCenter Server del clúster de confianza y los archivos de información del host de confianza al clúster de Trust Authority. Se da por sentado que está conectado a la instancia de vCenter Server del clúster de Trust Authority como administrador de Trust Authority. En la siguiente tabla, se muestran los componentes y los valores de ejemplo que se utilizan.

Tabla 9-7. Ejemplo de configuración de vSphere Trust Authority

Componente	Valor
Variable `$vTA`	`Get-TrustAuthorityCluster 'vTA Cluster1'`
vCenter Server para clúster de Trust Authority	192.168.210.22
Nombres de clústeres de Trust Authority	vTA Cluster1 (habilitado) vTA Cluster2 (deshabilitado)
Archivo de información principal	`C:\vta\principal.json`
Archivo de certificado de TPM	`C:\vta\cacert.cer`
Archivo de imagen base del host ESXi	`C:\vta\image.tgz`
Administrador de Trust Authority	trustedadmin@vsphere.local

```
PS C:\Users\Administrator> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.210.22                  443  VSPHERE.LOCAL\trustedadmin

PS C:\Users\Administrator> Get-TrustAuthorityCluster

Name                 State                Id
----                 -----                --
vTA Cluster1         Enabled              TrustAuthorityCluster-domain-c8
vTA Cluster2         Disabled             TrustAuthorityCluster-domain-c26

PS C:\Users\Administrator> $vTA = Get-TrustAuthorityCluster 'vTA Cluster1'

PS C:\Users\Administrator.CORP> New-TrustAuthorityPrincipal -TrustAuthorityCluster $vTA
-FilePath C:\vta\principal.json

Name                                           Domain          Type
TrustAuthorityClusterId
```

```
----                                         ------          ----
-----------------------
vpxd-de207929-0601-43ef-9616-47d0cee0302f     vsphere.local   STS_USER
TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator.CORP> Get-TrustAuthorityPrincipal -TrustAuthorityCluster $vTA

Name                                         Domain          Type
TrustAuthorityClusterId
----                                         ------          ----
-----------------------
vpxd-de207929-0601-43ef-9616-47d0cee0302f     vsphere.local   STS_USER
TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator.CORP> New-TrustAuthorityTpm2CACertificate -TrustAuthorityCluster
$vTA -FilePath C:\vta\cacert.cer

TrustAuthorityClusterId                 Name                                     Health
-----------------------                 ----                                     ------
TrustAuthorityCluster-domain-c8         52BDB7B4B2F55C925C047257DED4588A7767D961 Ok

PS C:\Users\Administrator.CORP> New-TrustAuthorityVMHostBaseImage -TrustAuthorityCluster $vTA
-FilePath C:\vta\image.tgz

TrustAuthorityClusterId                 VMHostVersion                            Health
-----------------------                 -------------                            ------
TrustAuthorityCluster-domain-c8         ESXi 7.0.0-0.0.14828939                  Ok
```

Pasos siguientes

Continúe con Crear el proveedor de claves en el clúster de Trust Authority.

Crear el proveedor de claves en el clúster de Trust Authority

Para que el servicio de proveedor de claves se conecte a un proveedor de claves, primero debe crear un proveedor de claves de confianza y, a continuación, establecer una configuración de confianza entre el clúster de vSphere Trust Authority y el servidor de claves (Key Management Server, KMS). Para la mayoría de los servidores de claves que cumplen con KMIP, esta configuración implica el establecimiento de certificados de cliente y servidor.

Lo que antes se denominaba clúster KMS en vSphere 6.7 ahora se denomina proveedor de claves en vSphere 7.0 y versiones posteriores. Para obtener más información sobre los proveedores de claves, consulte Descripción del servicio de proveedor de claves de vSphere Trust Authority.

En un entorno de producción, puede crear varios proveedores de claves. Al crear varios proveedores de claves, puede abordar el modo en que se administra la implementación en función de la organización de la empresa, diferentes unidades de negocio o clientes, etc.

Si sigue estas tareas en orden, aún está conectado a la instancia de vCenter Server del clúster de vSphere Trust Authority.

Requisitos previos

- Habilitar el administrador de Trust Authority.
- Habilitar el estado de Trust Authority.
- Recopilar información sobre hosts ESXi e instancias de vCenter Server que serán de confianza.
- Importar la información del host de confianza en el clúster de Trust Authority.
- Cree y active una clave en el servidor de claves para que sea la clave principal del proveedor de claves de confianza. Esta clave envuelve otras claves y secretos utilizados por este proveedor de claves de confianza. Consulte la documentación del proveedor del servidor de claves para obtener más información sobre la creación de claves.

Procedimiento

1 Asegúrese de estar conectado a la instancia de vCenter Server del clúster de Trust Authority. Por ejemplo, puede introducir `$global:defaultviservers` para mostrar todos los servidores conectados.

2 (opcional) Si es necesario, puede ejecutar los siguientes comandos para asegurarse de que está conectado a la instancia de vCenter Server del clúster de Trust Authority.

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

3 Para crear el proveedor de claves de confianza, ejecute el cmdlet `New-TrustAuthorityKeyProvider`.

   Por ejemplo, este comando utiliza `1` para PrimaryKeyID y el nombre `clkp`. Si sigue estas tareas en orden, ya asignó la información de `Get-TrustAuthorityCluster` a una variable (por ejemplo, `$vTA = Get-TrustAuthorityCluster 'vTA Cluster'`).

```
New-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA -PrimaryKeyId 1 -Name clkp
-KmipServerAddress ip_address
```

   El valor de PrimaryKeyID suele ser un identificador de clave procedente del servidor de claves con un formato de UUID. No utilice el nombre de clave para PrimaryKeyID. El valor de PrimaryKeyID depende del proveedor. Consulte la documentación del servidor de claves. El cmdlet `New-TrustAuthorityKeyProvider` puede admitir otras opciones, como `KmipServerPort`, `ProxyAddress` y `ProxyPort`. Consulte el sistema de ayuda de `New-TrustAuthorityKeyProvider` para obtener más información.

   Cada proveedor de claves lógico, independientemente de su tipo (proveedor de claves estándar, de confianza y nativo), debe tener un nombre único en todos los sistemas vCenter Server.

Para obtener más información, consulte Nomenclatura de proveedor de claves.

Nota Para agregar varios servidores de claves al proveedor de claves, utilice el cmdlet `Add-TrustAuthorityKeyProviderServer`.

Se muestra la información del proveedor de claves.

4 Establezca la conexión de confianza para que el servidor de claves confíe en el proveedor de claves de confianza. El proceso exacto depende de los certificados que el proveedor de claves acepte y de la directiva de su empresa. Seleccione la opción adecuada para el servidor y finalice los pasos.

Opción	Consulte
Cargar certificado de cliente	Cargar el certificado de cliente para establecer una conexión de confianza con un proveedor de claves de confianza.
Cargar certificado y clave privada de KMS	Cargar el certificado y la clave privada para establecer una conexión de confianza con un proveedor de claves de confianza.
Nueva solicitud de firma de certificado	Crear una solicitud de firma del certificado para establecer una conexión de confianza con un proveedor de claves de confianza.

5 Para finalizar la configuración de confianza, cargue un certificado de servidor de claves para que el proveedor de claves de confianza confíe en el servidor de claves.

   a Asigne la información de `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA` a una variable.

      Por ejemplo:

      ```
      $kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
      ```

      Esta variable obtiene los proveedores de claves de confianza del clúster de Trust Authority especificado (en este caso, `$vTA`).

      Nota Si tiene más de un proveedor de claves de confianza, utilice comandos similares a los que se indican a continuación para seleccionar el que desee:

      ```
      Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
      <The trusted key providers listing is displayed.>
      $kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
      ```

      Al utilizar `Select-Object -Last 1`, se selecciona el último proveedor de claves de confianza de la lista.

   b Para obtener el certificado del servidor de claves, ejecute el comando `Get-TrustAuthorityKeyProviderServerCertificate`.

      Por ejemplo:

      ```
      Get-TrustAuthorityKeyProviderServerCertificate -KeyProviderServer
      $kp.KeyProviderServers
      ```

      Se mostrará la información del certificado de servidor. Inicialmente, el certificado no es de confianza, por lo que el estado de confianza es False. Si tiene más de un servidor de claves configurado, se devuelve una lista de certificados. Compruebe y agregue cada certificado siguiendo las instrucciones que se indican a continuación.

c Antes de confiar en el certificado, asigne la información de `Get-TrustAuthorityKeyProviderServerCertificate -KeyProviderServer $kp.KeyProviderServers` a una variable (por ejemplo, `cert`), ejecute el comando `$cert.Certificate.ToString()` y compruebe los resultados.

Por ejemplo:

```
$cert = Get-TrustAuthorityKeyProviderServerCertificate -KeyProviderServer
$kp.KeyProviderServers
$cert.Certificate.ToString()
```

Se muestra información del certificado, como el asunto, el emisor y demás datos.

d Para agregar el certificado del servidor KMIP al proveedor de claves de confianza, ejecute `Add-TrustAuthorityKeyProviderServerCertificate`.

Por ejemplo:

```
Add-TrustAuthorityKeyProviderServerCertificate -ServerCertificate $cert
```

Se mostrará la información del certificado y el estado de confianza ahora es True.

6 Compruebe el estado del proveedor de claves.

a Para actualizar el estado del proveedor de claves, reasigne la variable `$kp`.

Por ejemplo:

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

Nota Si tiene más de un proveedor de claves de confianza, utilice comandos similares a los que se indican a continuación para seleccionar el que desee:

```
Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
<The trusted key providers listing is displayed.>
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
```

Al utilizar `Select-Object -Last 1`, se selecciona el último proveedor de claves de confianza de la lista.

b Ejecute el comando `$kp.Status` para obtener el estado del proveedor de claves.

Por ejemplo:

```
$kp.Status
```

Nota El estado puede tardar unos minutos en actualizarse. Para ver el estado, reasigne la variable `$kp` y vuelva a ejecutar el comando `$kp.Status`.

Si el estado de mantenimiento es Ok, quiere decir que el proveedor de claves se está ejecutando correctamente.

Resultados

El proveedor de claves de confianza se creará y se establecerá una relación de confianza con el servidor de claves.

Ejemplo: Crear el proveedor de claves en el clúster de Trust Authority

En este ejemplo se muestra cómo utilizar PowerCLI para crear el proveedor de claves de confianza en el clúster de Trust Authority. Se da por sentado que está conectado a la instancia de vCenter Server del clúster de Trust Authority como administrador de Trust Authority. También utiliza un certificado firmado por el proveedor del servidor de claves después de enviar una CSR al proveedor.

En la siguiente tabla, se muestran los componentes y los valores de ejemplo que se utilizan.

Tabla 9-8. Ejemplo de configuración de vSphere Trust Authority

Componente	Valor
Variable `$vTA`	`Get-TrustAuthorityCluster 'vTA Cluster'`
Variable `$kp`	`Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA`
Variable `$cert`	`Get-TrustAuthorityKeyProviderServerCertificate -KeyProviderServer $kp.KeyProviderServers`
vCenter Server para clúster de Trust Authority	192.168.210.22
Servidor de claves que cumple con KMIP	192.168.110.91
Usuario del servidor de claves que cumple con KMIP	vcqekmip
Nombre del clúster de Trust Authority	Clúster de vTA
Administrador de Trust Authority	trustedadmin@vsphere.local

```
PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

PS C:\Users\Administrator.CORP> New-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
-PrimaryKeyId 8 -Name clkp -KmipServerAddress 192.168.110.91
Name                 PrimaryKeyId         Type       TrustAuthorityClusterId
----                 ------------         ----       -----------------------
clkp                 8                    KMIP       TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator.CORP> New-TrustAuthorityKeyProviderClientCertificate -KeyProvider
$kp
<Export the client certificate when you need to use it.>
PS C:\Users\Administrator.CORP> Export-TrustAuthorityKeyProviderClientCertificate
-KeyProvider $kp -FilePath clientcert.pem

PS C:\Users\Administrator.CORP> $kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster
$vTA
PS C:\Users\Administrator.CORP> Get-TrustAuthorityKeyProviderServerCertificate
```

```
-KeyProviderServer $kp.KeyProviderServers

Certificate                         Trusted    KeyProviderServerId       KeyProviderId
-----------                         -------    -------------------       -------------
[Subject]...                        False      domain-c8-clkp:192.16.... domain-c8-clkp

PS C:\WINDOWS\system32> $cert.Certificate.ToString()
[Subject]
  E=<domain>, CN=<IP address>, OU=VMware Engineering, O=VMware, L=Palo Alto, S=California,
C=US

[Issuer]
  O=<host>.eng.vmware.com, C=US, DC=local, DC=vsphere, CN=CA

[Serial Number]
  00CEF192BBF9D80C9F

[Not Before]
  8/10/2015 4:16:12 PM

[Not After]
  8/9/2020 4:16:12 PM

[Thumbprint]
  C44068C124C057A3D07F51DCF18720E963604B70

PS C:\Users\Administrator.CORP> $cert = Get-TrustAuthorityKeyProviderServerCertificate
-KeyProviderServer $kp.KeyProviderServers
PS C:\Users\Administrator.CORP> Add-TrustAuthorityKeyProviderServerCertificate
-ServerCertificate $cert

Certificate                         Trusted    KeyProviderServerId       KeyProviderId
-----------                         -------    -------------------       -------------
[Subject]...                        True                                 domain-c8-clkp

PS C:\Users\Administrator.CORP> $kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster
$vTA
PS C:\Users\Administrator.CORP> $kp.Status

KeyProviderId Health HealthDetails ServerStatus
------------- ------ ------------- ------------
domain-c8-kp4     Ok {}            {192.168.210.22}
```

Pasos siguientes

Continúe con Exportar la información del clúster de Trust Authority.

Cargar el certificado de cliente para establecer una conexión de confianza con un proveedor de claves de confianza

Algunos proveedores de servidores de claves (KMS) requieren que usted cargue el certificado de cliente del proveedor de claves de confianza en el servidor de claves. Después de la carga, el servidor de claves acepta el tráfico que proviene del proveedor de claves de confianza.

Requisitos previos

- Habilitar el administrador de Trust Authority.
- Habilitar el estado de Trust Authority.
- Recopilar información sobre hosts ESXi e instancias de vCenter Server que serán de confianza.
- Importar la información del host de confianza en el clúster de Trust Authority.
- Crear el proveedor de claves en el clúster de Trust Authority.

Procedimiento

1 Asegúrese de estar conectado a la instancia de vCenter Server del clúster de Trust Authority. Por ejemplo, puede introducir `$global:defaultviservers` para mostrar todos los servidores conectados.

2 (opcional) Si es necesario, puede ejecutar los siguientes comandos para asegurarse de que está conectado a la instancia de vCenter Server del clúster de Trust Authority.

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

3 Asigne la información de `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA` a una variable.

Por ejemplo:

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

Si sigue estas tareas en orden, ya asignó la información de `Get-TrustAuthorityCluster` a una variable (por ejemplo, `$vTA = Get-TrustAuthorityCluster 'vTA Cluster'`).

Esta variable obtiene los proveedores de claves de confianza del clúster de Trust Authority especificado (en este caso, `$vTA`).

Nota Si tiene más de un proveedor de claves de confianza, utilice comandos similares a los que se indican a continuación para seleccionar el que desee:

```
Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
<The trusted key providers listing is displayed.>
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
```

Al utilizar `Select-Object -Last 1`, se selecciona el último proveedor de claves de confianza de la lista.

---

4 Para crear el certificado de cliente del proveedor de claves de confianza, ejecute el cmdlet `New-TrustAuthorityKeyProviderClientCertificate`.

   Por ejemplo:

```
New-TrustAuthorityKeyProviderClientCertificate -KeyProvider $kp
```

   Se mostrará la huella digital.

5 Para exportar el certificado de cliente del proveedor de claves, ejecute el cmdlet `Export-TrustAuthorityKeyProviderClientCertificate`.

   Por ejemplo:

```
Export-TrustAuthorityKeyProviderClientCertificate -KeyProvider $kp -FilePath clientcert.pem
```

   El certificado se exportará a un archivo.

6 Cargue el archivo de certificado en el servidor de claves.

   Consulte la documentación del servidor de claves para obtener más información.

Resultados

El proveedor de claves de confianza estableció una relación de confianza con el servidor de claves.

Cargar el certificado y la clave privada para establecer una conexión de confianza con un proveedor de claves de confianza

Algunos proveedores de servidores de claves (KMS) requieren que usted configure el proveedor de claves de confianza con el certificado de cliente y la clave privada proporcionados por el servidor de claves. Después de configurar el proveedor de claves de confianza, el servidor de claves acepta tráfico del proveedor de claves de confianza.

Requisitos previos

- Habilitar el administrador de Trust Authority.
- Habilitar el estado de Trust Authority.
- Recopilar información sobre hosts ESXi e instancias de vCenter Server que serán de confianza.
- Importar la información del host de confianza en el clúster de Trust Authority.
- Crear el proveedor de claves en el clúster de Trust Authority.

- Solicite un certificado y una clave privada en formato PEM al proveedor del servidor de claves. Si el certificado que se devuelve tiene un formato distinto a PEM, conviértalo a ese formato. Si la clave privada está protegida con una contraseña, cree un archivo PEM en el que la contraseña se haya eliminado. Puede usar el comando `openssl` para ambas operaciones. Por ejemplo:
  - Para convertir un certificado de formato CRT a PEM:

    ```
    openssl x509 -in clientcert.crt -out clientcert.pem -outform PEM
    ```

  - Para convertir un certificado de formato DER a PEM:

    ```
    openssl x509 -inform DER -in clientcert.der -out clientcert.pem
    ```

  - Realice lo siguiente para eliminar la contraseña de una clave privada:

    ```
    openssl rsa -in key.pem -out keynopassword.pem
    Enter pass phrase for key.pem:
    writing RSA key
    ```

Procedimiento

1 Asegúrese de estar conectado a la instancia de vCenter Server del clúster de Trust Authority. Por ejemplo, puede introducir `$global:defaultviservers` para mostrar todos los servidores conectados.

2 (opcional) Si es necesario, puede ejecutar los siguientes comandos para asegurarse de que está conectado a la instancia de vCenter Server del clúster de Trust Authority.

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

3 Asigne la información de `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA` a una variable.

Por ejemplo:

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

Si sigue estas tareas en orden, ya asignó la información de `Get-TrustAuthorityCluster` a una variable (por ejemplo, `$vTA = Get-TrustAuthorityCluster 'vTA Cluster'`).

La variable `$kp` obtiene los proveedores de claves de confianza del clúster de Trust Authority especificado (en este caso, `$vTA`).

Nota Si tiene más de un proveedor de claves de confianza, utilice comandos similares a los que se indican a continuación para seleccionar el que desee:

```
Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
<The trusted key providers listing is displayed.>
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
```

Al utilizar `Select-Object -Last 1`, se selecciona el último proveedor de claves de confianza de la lista.

4 Cargue el certificado y la clave privada mediante el comando `Set-TrustAuthorityKeyProviderClientCertificate`.

Por ejemplo:

```
Set-TrustAuthorityKeyProviderClientCertificate -KeyProvider $kp -CertificateFilePath
<path/to/certfile.pem> -PrivateKeyFilePath <path/to/privatekey.pem>
```

Resultados

El proveedor de claves de confianza estableció una relación de confianza con el servidor de claves.

Crear una solicitud de firma del certificado para establecer una conexión de confianza con un proveedor de claves de confianza

Algunos proveedores del servidor de claves (Key Management Server, KMS) requieren que se genere una solicitud de firma del certificado (Certificate Signing Request, CSR) y se envíe al proveedor del servidor de claves. El proveedor del servidor de claves firma la CSR y devuelve el certificado firmado. Después de configurar este certificado firmado como certificado de cliente del proveedor de claves de confianza, el servidor de claves acepta el tráfico que proviene del proveedor de claves de confianza.

Esta tarea consta de dos pasos. Primero debe generar la CSR y enviarla al proveedor del servidor de claves. A continuación, cargue el certificado firmado que recibió del proveedor del servidor de claves.

Requisitos previos

- Habilitar el administrador de Trust Authority.
- Habilitar el estado de Trust Authority.
- Recopilar información sobre hosts ESXi e instancias de vCenter Server que serán de confianza.
- Importar la información del host de confianza en el clúster de Trust Authority.
- Crear el proveedor de claves en el clúster de Trust Authority.

Procedimiento

1 Asegúrese de estar conectado a la instancia de vCenter Server del clúster de Trust Authority. Por ejemplo, puede introducir `$global:defaultviservers` para mostrar todos los servidores conectados.

2 (opcional) Si es necesario, puede ejecutar los siguientes comandos para asegurarse de que está conectado a la instancia de vCenter Server del clúster de Trust Authority.

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

3 Asigne la información de `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA` a una variable.

Por ejemplo:

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

Si sigue estas tareas en orden, ya asignó la información de `Get-TrustAuthorityCluster` a una variable (por ejemplo, `$vTA = Get-TrustAuthorityCluster 'vTA Cluster'`).

Esta variable obtiene los proveedores de claves de confianza del clúster de Trust Authority especificado (en este caso, `$vTA`).

Nota Si tiene más de un proveedor de claves de confianza, utilice comandos similares a los que se indican a continuación para seleccionar el que desee:

```
Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
<The trusted key providers listing is displayed.>
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
```

Al utilizar `Select-Object -Last 1`, se selecciona el último proveedor de claves de confianza de la lista.

4 Para generar una CSR, utilice el cmdlet `New-TrustAuthorityKeyProviderClientCertificateCSR`.

Por ejemplo:

```
New-TrustAuthorityKeyProviderClientCertificateCSR -KeyProvider $kp
```

Se mostrará la CSR. También puede utilizar el cmdlet `Get-TrustAuthorityKeyProviderClientCertificateCSR -KeyProvider $kp` para obtener la CSR.

5 Para obtener un certificado firmado, envíe la CSR al proveedor del servidor de claves.

El certificado debe estar en formato PEM. Si el certificado que se devuelve tiene un formato distinto a PEM, conviértalo a ese formato mediante el comando `openssl`. Por ejemplo:

- Para convertir un certificado de formato CRT a PEM:

```
openssl x509 -in clientcert.crt -out clientcert.pem -outform PEM
```

- Para convertir un certificado de formato DER a PEM:

```
openssl x509 -inform DER -in clientcert.der -out clientcert.pem
```

6 Cuando se reciba el certificado firmado del proveedor del servidor de claves, cárguelo en el servidor de claves mediante el cmdlet `Set-TrustAuthorityKeyProviderClientCertificate`.

Por ejemplo:

```
Set-TrustAuthorityKeyProviderClientCertificate -KeyProvider $kp -CertificateFilePath
<path/tp/certfile.pem>
```

Resultados

El proveedor de claves de confianza estableció una relación de confianza con el servidor de claves.

Exportar la información del clúster de Trust Authority

Respecto al clúster de confianza que se va a conectar al clúster de vSphere Trust Authority, debe exportar la información del servicio del clúster de Trust Authority como un archivo y, a continuación, importar dicho archivo al clúster de confianza. Debe asegurarse de mantener la confidencialidad de este archivo y de transportarlo de forma segura.

Si sigue estas tareas en orden, aún está conectado a la instancia de vCenter Server del clúster de Trust Authority.

Nota Almacene el archivo de información del servicio en una ubicación segura, en caso de que deba restaurar la configuración de vSphere Trust Authority.

Requisitos previos

- Habilitar el administrador de Trust Authority.
- Habilitar el estado de Trust Authority.
- Recopilar información sobre hosts ESXi e instancias de vCenter Server que serán de confianza.
- Importar la información del host de confianza en el clúster de Trust Authority.
- Crear el proveedor de claves en el clúster de Trust Authority.

Procedimiento

1 Asegúrese de estar conectado a la instancia de vCenter Server del clúster de Trust Authority. Por ejemplo, puede introducir `$global:defaultviservers` para mostrar todos los servidores conectados.

2 (opcional) Si es necesario, puede ejecutar los siguientes comandos para asegurarse de que está conectado a la instancia de vCenter Server del clúster de Trust Authority.

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

3 Para exportar el servicio de atestación del clúster de Trust Authority y la información del servicio de proveedor de claves, ejecute el cmdlet `Export-TrustAuthorityServicesInfo`.

Por ejemplo, este comando exporta la información del servicio al archivo `clsettings.json`. Si sigue estas tareas en orden, ya asignó la información de `Get-TrustAuthorityCluster` a una variable (por ejemplo, `$vTA = Get-TrustAuthorityCluster 'vTA Cluster'`).

```
Export-TrustAuthorityServicesInfo -TrustAuthorityCluster $vTA -FilePath
C:\vta\clsettings.json
```

Se creará el archivo.

Resultados

Se creará un archivo que contiene la información del clúster de Trust Authority.

Ejemplo: Exportar la información del clúster de Trust Authority

En este ejemplo se muestra cómo usar PowerCLI para exportar la información del servicio del clúster de Trust Authority. En la siguiente tabla, se muestran los componentes y los valores de ejemplo que se utilizan.

Tabla 9-9. Ejemplo de configuración de vSphere Trust Authority

Componente	Valor
Variable `$vTA`	`Get-TrustAuthorityCluster 'vTA Cluster'`
vCenter Server para clúster de Trust Authority	192.168.210.22
Administrador de Trust Authority	trustedadmin@vsphere.local

```
PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

PS C:\Users\Administrator.CORP> Export-TrustAuthorityServicesInfo -TrustAuthorityCluster $vTA
-FilePath C:\vta\clsettings.json

Mode                LastWriteTime         Length Name
```

```
----              -------------        ------ ----
-a----       10/16/2019   9:59 PM           8177 clsettings.json
```

Pasos siguientes

Continúe con Importar la información del clúster de Trust Authority en los hosts de confianza.

Importar la información del clúster de Trust Authority en los hosts de confianza

Después de importar la información del clúster de vSphere Trust Authority al clúster de confianza, los hosts de confianza inician el proceso de atestación con el clúster de Trust Authority.

Requisitos previos

- Habilitar el administrador de Trust Authority.
- Habilitar el estado de Trust Authority.
- Recopilar información sobre hosts ESXi e instancias de vCenter Server que serán de confianza.
- Importar la información del host de confianza en el clúster de Trust Authority.
- Crear el proveedor de claves en el clúster de Trust Authority.
- Exportar la información del clúster de Trust Authority.

Procedimiento

1 Asegúrese de que está conectado como administrador de Trust Authority a la instancia de vCenter Server del clúster de confianza.

   Por ejemplo, puede introducir `$global:defaultviservers` para mostrar todos los servidores conectados.

2 (opcional) Si es necesario, puede ejecutar los siguientes comandos para asegurarse de que está conectado a la instancia de vCenter Server del clúster de confianza.

   ```
   Disconnect-VIServer -server * -Confirm:$false
   Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password
   'password'
   ```

   Nota Como alternativa, puede iniciar otra sesión de PowerCLI para conectarse a la instancia de vCenter Server del clúster de confianza.

3 Compruebe que el estado del clúster de confianza está deshabilitado.

   ```
   Get-TrustedCluster
   ```

   El estado se muestra como Deshabilitado.

4 Asigne la información de `Get-TrustedCluster` a una variable.

Por ejemplo, este comando asigna información del clúster `Trusted Cluster` a la variable `$TC`.

```
$TC = Get-TrustedCluster -Name 'Trusted Cluster'
```

5 Compruebe el valor de la variable mediante eco.

Por ejemplo:

```
$TC
```

Se muestra la información de `Get-TrustedCluster`.

6 Para importar la información del clúster de Trust Authority a vCenter Server, ejecute el cmdlet `Import-TrustAuthorityServicesInfo`.

Por ejemplo, este comando importa la información del servicio desde el archivo `clsettings.json` exportado previamente en Exportar la información del clúster de Trust Authority.

```
Import-TrustAuthorityServicesInfo -FilePath C:\vta\clsettings.json
```

El sistema responde con un mensaje de confirmación.

```
Confirmation
Importing the TrustAuthorityServicesInfo into Server 'ip_address'. Do you want to proceed?

[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
```

7 En la solicitud de confirmación, presione Intro. (El valor predeterminado es **Y**).

Se muestra la información del servicio de los hosts en el clúster de Trust Authority.

8 Para habilitar el clúster de confianza, ejecute el cmdlet `Set-TrustedCluster`.

Por ejemplo:

```
Set-TrustedCluster -TrustedCluster $TC -State Enabled
```

El sistema responde con un mensaje de confirmación.

```
Confirmation
Setting TrustedCluster 'cluster' with new TrustedState 'Enabled'. Do you want to proceed?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
```

Si el clúster de confianza no se encuentra en un estado correcto, se muestra el siguiente mensaje de advertencia antes del mensaje de confirmación:

```
WARNING: The TrustedCluster 'cluster' is not healthy in its TrustedClusterAppliedStatus.
This cmdlet will automatically remediate the TrustedCluster.
```

9 En la solicitud de confirmación, presione Intro. (El valor predeterminado es **Y**).

Se habilita el clúster de confianza.

Nota También puede habilitar el clúster de confianza mediante la habilitación del servicio de atestación y el servicio del proveedor de claves de forma individual. Utilice los comandos`Add-TrustedClusterAttestationServiceInfo` y`Add-TrustedClusterKeyProviderServiceInfo`. Por ejemplo, los siguientes comandos habilitan los servicios de uno en uno en el clúster de `Trusted Cluster`, que tiene dos servicios de proveedor de claves y dos servicios de atestación.

```
Add-TrustedClusterAttestationServiceInfo -TrustedCluster 'Trusted Cluster'
-AttestationServiceInfo (Get-AttestationServiceInfo | Select-Object -index 0,1)
Add-TrustedClusterKeyProviderServiceInfo  -TrustedCluster 'Trusted Cluster'
-KeyProviderServiceInfo (Get-KeyProviderServiceInfo | Select-Object -index 0,1)
```

---

10 Compruebe que el servicio de atestación y el servicio de proveedor de claves estén configurados en el clúster de confianza.

   a Asigne la información de `Get-TrustedCluster` a una variable.

   Por ejemplo, este comando asigna información del clúster `Trusted Cluster` a la variable `$TC`.

   ```
   $TC = Get-TrustedCluster -Name 'Trusted Cluster'
   ```

   b Compruebe que el servicio de atestación está configurado.

   ```
   $tc.AttestationServiceInfo
   ```

   Se mostrará la información del servicio de atestación.

   c Compruebe que el servicio de proveedor de claves está configurado.

   ```
   $tc.KeyProviderServiceInfo
   ```

   Se mostrará la información del servicio de proveedor de claves.

Resultados

Los hosts ESXi de confianza del clúster de confianza inician el proceso de atestación con el clúster de Trust Authority.

Ejemplo: Importar la información del clúster de Trust Authority en los hosts de confianza

En este ejemplo, se muestra cómo importar la información del servicio del clúster de Trust Authority en el clúster de confianza. En la siguiente tabla, se muestran los componentes y los valores de ejemplo que se utilizan.

Tabla 9-10. Ejemplo de configuración de vSphere Trust Authority

Componente	Valor
vCenter Server del clúster de confianza	192.168.110.22
Administrador de Trust Authority	trustedadmin@vsphere.local
Nombre del clúster de confianza	Clúster de confianza
Hosts ESXi en el clúster de Trust Authority	192.168.210.51 y 192.168.210.52
Variable `$TC`	`Get-TrustedCluster -Name 'Trusted Cluster'`

```
PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.110.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.110.22                 443   VSPHERE.LOCAL\trustedadmin

PS C:\Users\Administrator.CORP> Get-TrustedCluster

Name                 State             Id
----                 -----             --
Trusted Cluster      Disabled          TrustedCluster-domain-c8

PS C:\Users\Administrator.CORP> $TC = Get-TrustedCluster -Name 'Trusted Cluster'
PS C:\Users\Administrator.CORP> $TC

Name                 State             Id
----                 -----             --
Trusted Cluster      Disabled          TrustedCluster-domain-c8

PS C:\Users\Administrator.CORP> Import-TrustAuthorityServicesInfo -FilePath
C:\vta\clsettings.json

Confirmation
Importing the TrustAuthorityServicesInfo into Server '192.168.110.22'. Do you want to proceed?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): y

ServiceAddress                 ServicePort          ServiceGroup
--------------                 -----------          ------------
192.168.210.51                 443                  host-13:86f7ab6c-ad6f-4606-...
192.168.210.52                 443                  host-16:86f7ab6c-ad6f-4606-...
192.168.210.51                 443                  host-13:86f7ab6c-ad6f-4606-...
192.168.210.52                 443                  host-16:86f7ab6c-ad6f-4606-...

PS C:\Users\Administrator.CORP> Set-TrustedCluster -TrustedCluster $TC -State Enabled

Confirmation
Setting TrustedCluster 'Trusted Cluster' with new TrustedState 'Enabled'. Do you want to
proceed?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
```

```
Name                 State            Id
----                 -----            --
Trusted Cluster      Enabled          TrustedCluster-domain-c8

PS C:\Users\Administrator.CORP> $TC = Get-TrustedCluster -Name 'Trusted Cluster'
PS C:\Users\Administrator.CORP> $tc.AttestationServiceInfo

ServiceAddress                ServicePort         ServiceGroup
--------------                -----------         ------------
192.168.210.51                443                 host-13:dc825986-73d2-463c-...
192.168.210.52                443                 host-16:dc825986-73d2-463c-...

PS C:\Users\Administrator.CORP> $tc.KeyProviderServiceInfo

ServiceAddress                ServicePort         ServiceGroup
--------------                -----------         ------------
192.168.210.51                443                 host-13:dc825986-73d2-463c-...
192.168.210.52                443                 host-16:dc825986-73d2-463c-...
```

Pasos siguientes

Continúe con Configurar el proveedor de claves de confianza para hosts de confianza mediante vSphere Client o Configurar el proveedor de claves de confianza para hosts de confianza mediante la línea de comandos.

Configurar el proveedor de claves de confianza para hosts de confianza mediante vSphere Client

Puede configurar el proveedor de claves de confianza mediante vSphere Client.

Requisitos previos

- Habilitar el administrador de Trust Authority.
- Habilitar el estado de Trust Authority.
- Recopilar información sobre hosts ESXi e instancias de vCenter Server que serán de confianza.
- Importar la información del host de confianza en el clúster de Trust Authority.
- Crear el proveedor de claves en el clúster de Trust Authority.
- Exportar la información del clúster de Trust Authority.
- Importar la información del clúster de Trust Authority en los hosts de confianza.

Procedimiento

1 Conéctese a la instancia de vCenter Server del clúster de confianza mediante vSphere Client.

2 Inicie sesión como administrador de vCenter Server o como un administrador con el privilegio **Operaciones criptográficas.Administrar servidores de claves**.

3 Seleccione la instancia de vCenter Server y, a continuación, seleccione **Configurar**.

4 Seleccione **Proveedores de claves** en **Seguridad**.

5 Seleccione **Agregar proveedores de claves de confianza**.

Los proveedores de claves de confianza que están disponibles se muestran con el estado de conectado.

6 Seleccione un proveedor de claves de confianza y haga clic en **Agregar proveedores de claves**.

El proveedor de claves de confianza se muestra como De confianza y Conectado. Si este es el primer proveedor de claves de confianza que agrega, se marcará como predeterminado.

Nota Se necesita un tiempo para que todos los hosts puedan obtener el proveedor de claves y para que el vCenter Server actualice su memoria caché. Debido a la forma en que se propaga la información, es posible que deba esperar unos minutos para utilizar el proveedor de claves para operaciones de claves en algunos de los hosts.

Resultados

Ahora, los hosts ESXi de confianza podrán realizar operaciones criptográficas, como crear máquinas virtuales cifradas.

Pasos siguientes

El cifrado de una máquina virtual con un proveedor de claves de confianza tiene el mismo aspecto que la experiencia de usuario de cifrado de máquinas virtuales que se proporcionó por primera vez en vSphere 6.5. Consulte Capítulo 10 Usar el cifrado en el entorno de vSphere.

Configurar el proveedor de claves de confianza para hosts de confianza mediante la línea de comandos

Puede configurar proveedores de claves de confianza mediante la línea de comandos. Puede configurar el proveedor de claves de confianza predeterminado de vCenter Server o en el nivel del clúster o de carpeta de clúster en la jerarquía de objetos de vCenter.

Requisitos previos

- Habilitar el administrador de Trust Authority.
- Habilitar el estado de Trust Authority.
- Recopilar información sobre hosts ESXi e instancias de vCenter Server que serán de confianza.
- Importar la información del host de confianza en el clúster de Trust Authority.
- Crear el proveedor de claves en el clúster de Trust Authority.
- Exportar la información del clúster de Trust Authority.
- Importar la información del clúster de Trust Authority en los hosts de confianza.

En el clúster de confianza, debe tener una función que incluya el privilegio **Operaciones de cifrado.Administrar KMS**.

Procedimiento

1 Asegúrese de que está conectado como administrador a la instancia de vCenter Server del clúster de confianza.

   Por ejemplo, puede introducir `$global:defaultviservers` para mostrar todos los servidores conectados.

2 (opcional) Si es necesario, puede ejecutar los siguientes comandos para asegurarse de que está conectado a la instancia de vCenter Server del clúster de confianza.

   ```
   Disconnect-VIServer -server * -Confirm:$false
   Connect-VIServer -server TrustedCluster_VC_ip_address -User admin_user -Password 'password'
   ```

3 Obtenga el proveedor de claves de confianza.

   ```
   Get-KeyProvider
   ```

   Puede usar la opción `-Name` *keyprovider* para especificar un único proveedor de claves de confianza.

4 Asigne la información de proveedor de claves de confianza de `Get-KeyProvider` a una variable.

   Por ejemplo, este comando asigna la información a la variable `$workload_kp`.

   ```
   $workload_kp = Get-KeyProvider
   ```

   Si cuenta con varios proveedores de claves de confianza, puede utilizar `Select-Object` para seleccionar uno de ellos.

   ```
   $workload_kp = Get-KeyProvider | Select-Object -Index 0
   ```

5 Registre el proveedor de claves de confianza.

   ```
   Register-KeyProvider -KeyProvider $workload_kp
   ```

   Para registrar proveedores de claves de confianza adicionales, repita los pasos 4 y 5.

   Nota Se necesita un tiempo para que todos los hosts puedan obtener el proveedor de claves y para que el vCenter Server actualice su memoria caché. Debido a la forma en que se propaga la información, es posible que deba esperar unos minutos para utilizar el proveedor de claves para operaciones de claves en algunos de los hosts.

6 Establezca el proveedor de claves de confianza predeterminado que se utilizará.

   a Para establecer el proveedor de claves predeterminado en el nivel de vCenter Server, ejecute el siguiente comando.

```
Set-KeyProvider -KeyProvider $workload_kp -DefaultForSystem
```

   b Para establecer el proveedor de claves en el nivel de clúster, ejecute el siguiente comando.

   Por ejemplo, este comando establece el proveedor de claves del clúster `Trusted Cluster`.

```
Add-EntityDefaultKeyProvider -KeyProvider $workload_kp -Entity 'Trusted Cluster'
```

   c Para establecer el proveedor de claves en el nivel de carpeta del clúster, ejecute el siguiente comando.

   Por ejemplo, este comando establece el proveedor de claves de la carpeta de clúster `TC Folder`, que se creó en el centro de datos de `workLoad`.

```
Add-EntityDefaultKeyProvider -KeyProvider $workload_kp -Entity 'TC Folder'
```

Pasos siguientes

El cifrado de una máquina virtual con un proveedor de claves de confianza tiene el mismo aspecto que la experiencia de usuario de cifrado de máquinas virtuales que se proporcionó por primera vez en vSphere 6.5. Consulte Capítulo 10 Usar el cifrado en el entorno de vSphere.

Administrar vSphere Trust Authority en su entorno vSphere

Después de configurar vSphere Trust Authority, puede realizar otras operaciones, como detener e iniciar servicios, agregar hosts a clústeres y ver el estado del clúster de Trust Authority.

Puede realizar tareas mediante vSphere Client, la API y los cmdlets de PowerCLI. Consulte *Guía de programación de vSphere Web Services SDK*, la documentación de *VMware PowerCLI* y la documentación de *Referencia de cmdlets de VMware PowerCLI*.

Iniciar, detener y reiniciar los servicios de vSphere Trust Authority

Puede iniciar, detener y reiniciar los servicios de vSphere Trust Authority mediante vSphere Client.

Los servicios que componen vSphere Trust Authority son el servicio de atestación (attestd) y el servicio de proveedor de claves (kmxd).

Procedimiento

1 Conéctese a la instancia de vCenter Server del clúster de vSphere Trust Authority mediante vSphere Client.

2 Inicie sesión como administrador.

3 Desplácese hasta un host ESXi en el clúster de Trust Authority.

4 Seleccione **Configurar** y, luego, seleccione **Servicios** en **Sistema**.

5 Busque el servicio attestd y el servicio kmxd.

6 Seleccione la operación **Reiniciar**, **Iniciar** o **Detener** según corresponda.

Ver los hosts de Trust Authority

Puede ver los hosts de vSphere Trust Authority configurados para un clúster de confianza mediante vSphere Client.

Procedimiento

1 Conéctese a la instancia de vCenter Server del clúster de confianza mediante vSphere Client.

2 Inicie sesión como administrador.

3 Seleccione la instancia de vCenter Server.

4 Haga clic en la pestaña **Configurar** y seleccione **Trust Authority** en **Seguridad**.

   Aparecerán los hosts ESXi del clúster de Trust Authority configurados para el clúster de confianza.

Ver el estado del clúster de vSphere Trust Authority

Puede ver el estado del clúster de vSphere Trust Authority mediante vSphere Client. El estado puede ser habilitado o deshabilitado.

Cuando el estado del clúster de Trust Authority es habilitado, los hosts de confianza del clúster de confianza pueden comunicarse con el servicio de atestación y con el servicio de proveedor de claves.

Procedimiento

1 Conéctese a la instancia de vCenter Server del clúster de Trust Authority mediante vSphere Client.

2 Inicie sesión como administrador.

3 Seleccione el clúster de Trust Authority en la jerarquía de objetos.

4 Haga clic en la pestaña **Configurar** y seleccione **Clúster de Trust Authority** en **Trust Authority**.

   El estado se muestra como Habilitado o Deshabilitado.

Reiniciar el servicio de host de confianza

Puede reiniciar el servicio que se ejecuta en los hosts de confianza.

El servicio, kmxa, se ejecuta en los hosts de confianza ESXi.

Requisitos previos

Se debe habilitar el acceso a ESXi Shell. Consulte Activar el acceso a ESXi Shell mediante vSphere Client.

Procedimiento

1 Utilice SSH u otra conexión de consola remota para iniciar una sesión en host de confianza ESXi.

2 Inicie sesión como raíz.

3 Ejecute el siguiente comando.

```
/etc/init.d/kmxa restart
```

Agregar y eliminar hosts de vSphere Trust Authority

Puede agregar hosts ESXi a un clúster de vSphere Trust Authority o eliminarlos de ellos mediante scripts suministrados por VMware.

En vSphere 7.0, puede agregar hosts ESXi a un clúster de vSphere Trust Authority o a un clúster de confianza existente, así como eliminarlos de ellos, mediante scripts suministrados por VMware. En vSphere 7.0 Update 1 y versiones posteriores, se utiliza la función de corrección para agregar hosts ESXi a un clúster de confianza. Consulte Agregar un host a un clúster de confianza mediante vSphere Client y Agregar un host a un clúster de confianza mediante la línea de comandos.

En vSphere 7.0 Update 1 y versiones posteriores, aún hay que utilizar scripts para agregar hosts ESXi a un clúster de Trust Authority existente. Consulte los artículos de la base de conocimientos de VMware en https://kb.vmware.com/s/article/77234 y https://kb.vmware.com/s/article/77146.

Agregar un host a un clúster de confianza mediante vSphere Client

Es posible agregar hosts ESXi a un clúster de confianza existente mediante vSphere Client.

Después de configurar inicialmente un clúster de confianza, es posible que desee agregar más hosts ESXi. Sin embargo, en caso de agregar el host a un clúster de confianza, debe realizar el paso adicional de corrección. Cuando corrija el clúster de confianza, debe asegurarse de que el estado de configuración deseado coincida con la configuración aplicada.

En la primera versión de vSphere Trust Authority publicada en vSphere 7.0, los scripts se ejecutan para agregar un host a un clúster de confianza existente. En vSphere 7.0 Update 1 y versiones posteriores, se utiliza la funcionalidad de corrección para agregar un host a un clúster de confianza. En vSphere 7.0 Update 1 y versiones posteriores, aún hay que utilizar scripts para agregar un host a un clúster de Trust Authority existente. Consulte Agregar y eliminar hosts de vSphere Trust Authority.

Requisitos previos

La instancia de vCenter Server para el clúster de confianza debe ejecutar vSphere 7.0 Update 1 o versiones posteriores.

Si se dispone a agregar un host ESXi que tenga otra versión de ESXi o un tipo de hardware de TPM diferente al que configuró inicialmente para el clúster de confianza, tendrá que realizar algunos pasos adicionales. Debe exportar e importar esta información en el clúster de vSphere Trust Authority. Consulte Recopilar información sobre hosts ESXi e instancias de vCenter Server que serán de confianza y Importar la información del host de confianza en el clúster de Trust Authority.

Privilegios necesarios: consulte las tareas de adición de hosts en Privilegios de vCenter Server necesarios para la realización de tareas comunes.

Procedimiento

1 Conéctese a la instancia de vCenter Server del clúster de confianza mediante vSphere Client.

2 Inicie sesión como administrador de Trust Authority.

3 Desplácese hasta un clúster de confianza.

4 En la pestaña **Configurar**, seleccione **Configuración > Inicio rápido**.

5 En la tarjeta **Agregar hosts**, haga clic en **Agregar**.

6 Siga las indicaciones.

7 En la pestaña **Trust Authority**, haga clic en **Corregir**.

8 Para comprobar que el clúster de confianza esté en buen estado, haga clic en **Comprobar estado**.

Agregar un host a un clúster de confianza mediante la línea de comandos

Es posible agregar hosts ESXi a un clúster de confianza existente mediante la línea de comandos.

Después de configurar inicialmente un clúster de confianza, es posible que desee agregar más hosts ESXi. Sin embargo, en caso de agregar el host a un clúster de confianza, debe realizar el paso adicional de corrección. Cuando corrija el clúster de confianza, debe asegurarse de que el estado de configuración deseado coincida con la configuración aplicada.

En la primera versión de vSphere Trust Authority publicada en vSphere 7.0, los scripts se ejecutan para agregar un host a un clúster de confianza existente. Desde vSphere 7.0 Update 1 y versiones posteriores, se utiliza la funcionalidad de corrección para agregar un host de confianza. En vSphere 7.0 Update 1 y versiones posteriores, aún hay que utilizar scripts para agregar un host a un clúster de Trust Authority existente. Consulte Agregar y eliminar hosts de vSphere Trust Authority.

Requisitos previos

- La instancia de vCenter Server para el clúster de confianza debe ejecutar vSphere 7.0 Update 1 o versiones posteriores.
- Se requiere PowerCLI 12.1.0 o posterior.
- Privilegios necesarios: consulte las tareas de adición de hosts en Privilegios de vCenter Server necesarios para la realización de tareas comunes.

Procedimiento

1 Use los pasos que suela llevar a cabo para agregar el host ESXi al clúster de confianza.

2 En una sesión de PowerCLI, ejecute el cmdlet `Connect-VIServer` para conectarse como administrador de Trust Authority a la instancia de vCenter Server del clúster de confianza.

```
Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password
'password'
```

3 Para comprobar el estado del clúster de confianza, ejecute el cmdlet `Get-TrustedClusterAppliedStatus` de PowerCLI.

```
Get-TrustedClusterAppliedStatus -TrustedCluster 'TrustedCluster'
```

4 Si el clúster de confianza no está en buen estado, ejecute el cmdlet `Set-TrustedCluster` con el parámetro `-Remediate`.

```
Set-TrustedCluster -TrustedCluster 'TrustedCluster' -Remediate
```

5 Para comprobar que el clúster de confianza esté en buen estado, vuelva a ejecutar el cmdlet `Get-TrustedClusterAppliedStatus`.

```
Get-TrustedClusterAppliedStatus -TrustedCluster 'TrustedCluster'
```

Retirar hosts de confianza de un clúster de confianza

Puede eliminar (o bien retirar) hosts de confianza de un clúster de confianza. Puede retirar uno o todos los hosts de confianza de un clúster de confianza, según el escenario.

Cuando se retira un host de confianza, la función de corrección establece el estado deseado del host de confianza en el clúster que no es de confianza al que se mueve. El host de confianza retirado se convierte en un host normal. El clúster de confianza (desde donde se movió el host de confianza) sigue teniendo la configuración de estado deseada y sigue funcionando como un clúster de confianza.

Cuando se quitan todos los hosts de confianza de un clúster de confianza, se retira el clúster de confianza. Elimine tanto la configuración de estado deseada como la configuración aplicada de los hosts de confianza y del clúster de confianza. A continuación, mueva todos los hosts de confianza a un clúster que no sea de confianza.

Puede volver a utilizar los hosts de confianza retirados en su entorno. Por ejemplo, los hosts se pueden reutilizar en una capacidad de infraestructura que no sea de confianza o como hosts de vSphere Trust Authority. Los hosts retirados se pueden utilizar en la misma instancia de vCenter Server o en otra instancia de vCenter Server diferente.

Para obtener más información sobre el estado y la configuración del clúster de confianza, consulte Comprobar y corregir el estado del clúster de confianza.

Requisitos previos

- La instancia de vCenter Server para el clúster de confianza debe ejecutar vSphere 7.0 Update 1 o versiones posteriores.
- Si utiliza PowerCLI, se requiere la versión 12.1.0 o una versión posterior.

Procedimiento

1. Conéctese a la instancia de vCenter Server del clúster de confianza mediante vSphere Client.
2. Inicie sesión como administrador de Trust Authority.
3. Desplácese hasta un clúster de confianza.
4. Decida cómo va a retirar los hosts de confianza del clúster de confianza.

<table>
<tr><th>Tarea</th><th>Pasos</th></tr>
<tr><td>Mantener el estado de configuración deseado del clúster de confianza y los hosts de confianza restantes</td><td>a Coloque los hosts en modo de mantenimiento y trasládelos a un clúster nuevo y vacío (es decir, el clúster no contiene hosts).
b Salga del modo de mantenimiento en los hosts.
c Para el nuevo clúster vacío (no el clúster de confianza), en la pestaña Trust Authority, haga clic en Corregir.

Con la corrección se elimina la configuración de confianza de los hosts desplazados. El clúster de confianza conserva su configuración de estado deseada.</td></tr>
<tr><td>Eliminar el estado de configuración deseado y el estado de configuración aplicado de todos los hosts de confianza</td><td>a En una sesión de PowerCLI, ejecute el cmdlet <code>Connect-VIServer</code> para conectarse como administrador de Trust Authority a la instancia de vCenter Server del clúster de confianza.

<code>Connect-VIServer -server TrustedCluster_VC_ip_address
-User trust_admin_user -Password 'password'</code>

b Ejecute el cmdlet <code>Set-TrustedCluster</code>, por ejemplo:

<code>Set-TrustedCluster -TrustedCluster 'TrustedCluster'
-State Disabled</code>

La configuración de infraestructura de confianza se elimina de todos los hosts de confianza y su configuración de estado deseada se elimina del clúster de confianza.
c Ponga todos los hosts en modo de mantenimiento y muévalos a otro clúster.
d Salga del modo de mantenimiento en los hosts.</td></tr>
</table>

5 Para comprobar que el clúster de confianza está en buen estado, haga clic en **Comprobar estado** en la pestaña **Trust Authority** del clúster de confianza.

Pasos siguientes

Si ya no tiene previsto atestar las versiones específicas de ESXi o el hardware de TPM en los hosts ESXi que se hayan retirado, actualice la configuración del clúster de Trust Authority para obtener una seguridad óptima. Consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/77146.

Realizar una copia de seguridad de la configuración de vSphere Trust Authority

Utilice los archivos que exportó al configurar vSphere Trust Authority como la copia de seguridad de Trust Authority. Puede utilizar estos archivos para restaurar una implementación de Trust Authority. Mantenga la confidencialidad de estos archivos de configuración y transpórtelos de forma segura.

La mayor parte de la información de configuración y estado de vSphere Trust Authority se almacena en los hosts ESXi de la base de datos de ConfigStore. La interfaz de administración de vCenter Server que utiliza para realizar una copia de seguridad de una instancia de vCenter Server no realiza una copia de seguridad de la información de configuración de vSphere Trust Authority. Si guarda y almacena de forma segura los archivos de configuración que exportó al configurar el entorno de vSphere Trust Authority, tendrá la información necesaria para restaurar una configuración de vSphere Trust Authority. Consulte Recopilar información sobre hosts ESXi e instancias de vCenter Server que serán de confianza si debe generar esta información.

Cambiar la clave principal de un proveedor de claves de confianza

Es posible cambiar la clave principal de un proveedor de claves de confianza; por ejemplo, cuando quiera rotar la clave principal que se utiliza.

Consulte Prácticas recomendadas de cifrado de máquinas virtuales para obtener instrucciones sobre el ciclo de vida de las claves.

Requisitos previos

Cree y active una clave en el servidor de claves (KMS) para utilizarla como nueva clave principal del proveedor de claves de confianza. Esta clave envuelve otras claves y secretos utilizados por este proveedor de claves de confianza. Consulte la documentación del proveedor de KMS para obtener más información sobre cómo crear claves.

Procedimiento

1 Ejecute el comando `Set-TrustAuthorityKeyProvider`.

Por ejemplo:

```
Set-TrustAuthorityKeyProvider -MasterKeyId Key-ID
```

2 Compruebe el estado del proveedor de claves.

a Asigne la información de `Get-TrustAuthorityCluster` a una variable.

Por ejemplo:

```
$vTA = Get-TrustAuthorityCluster 'vTA Cluster'
```

b Asigne la información de `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA` a una variable.

Por ejemplo:

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

c Ejecute `$kp.Status` para comprobar el estado del proveedor de claves.

Por ejemplo:

```
$kp.Status

KeyProviderId Health HealthDetails ServerStatus
------------- ------ ------------- ------------
domain-c8-kp4     Ok {}            {IP_address}
```

Si el estado de mantenimiento es Ok, quiere decir que el proveedor de claves se está ejecutando correctamente.

Resultados

La nueva clave principal se utilizará en cualquier nueva operación de cifrado. Los datos cifrados con la clave principal anterior se seguirán descifrando con la clave anterior.

Informes de atestación de host de confianza

En vSphere Trust Authority, vCenter Server comprueba e informa el estado de atestación de un host de confianza. Puede utilizar vSphere Client para ver el estado de atestación de los hosts de confianza.

Qué son los informes de atestación de vSphere Trust Authority

vSphere Trust Authority utiliza la atestación remota para que los hosts de confianza demuestren la autenticidad de su software arrancado. La atestación verifica que los hosts de confianza ejecutan software VMware auténtico o software de socio firmado por VMware. El servidor de vCenter Server del clúster de confianza se comunica con el host de confianza para obtener un informe de atestación interno. El informe de atestación especifica si el host de confianza ha atestado o no con el servicio de atestación que se ejecuta en el clúster de Trust Authority. Si no se ha atestado el host de confianza, el informe de atestación también especifica un mensaje de error. vSphere Client muestra el estado de atestación de un host de confianza y si vSphere Trust Authority o vCenter Server atestó el host.

Estado de atestación pasado

Un estado aprobado indica que el host de confianza ha atestado con un servicio de atestación de vSphere Trust Authority, y el informe de atestación interno está disponible para vCenter Server.

Estado de atestación con errores

El estado con errores indica que el host de confianza no se pudo atestar con ningún servicio de atestación de vSphere Trust Authority. El informe de atestación interno de vCenter Server contiene el error notificado por el servicio de atestación con el que el host de confianza ha intentado atestar.

Gestión de los hosts de confianza no atestados

Cuando un host de confianza no está atestado, las máquinas virtuales, incluidas las máquinas virtuales cifradas, que se ejecutan en el host de confianza continúan siendo accesibles. No se pueden encender máquinas virtuales en un host de confianza no atestado. Sin embargo, aún puede agregar máquinas virtuales sin cifrar. Cuando se no haya atestado un host de confianza, realice los pasos necesarios para resolver el problema de atestación. Consulte Solucionar problemas de atestación de host de confianza.

Varios hosts de Trust Authority e informes de atestación

Cuando se hayan configurado varios hosts de Trust Authority, puede que haya varios informes de atestación disponibles desde cada host. Cuando se informa del estado, vSphere Client muestra el estado del primer informe "atestado" que encuentra. Si no hay informes "atestados", vSphere Client muestra el error del primer informe "no atestado" que encuentra.

Incluso si configuró varios hosts de Trust Authority, vSphere Client muestra el estado y, potencialmente, un mensaje de error de un solo informe de atestación.

Ver el estado de atestación de un clúster de confianza

Puede ver el estado de atestación de un host de confianza mediante vSphere Client.

Requisitos previos

- Tanto los hosts de confianza como los hosts de vSphere Trust Authority deben ejecutar ESXi 7.0 Update 1 o una versión posterior.
- Los hosts de vCenter Server para los clústeres correspondientes deben ejecutar vSphere 7.0 Update 1 o una versión posterior.

Procedimiento

1 Conéctese a la instancia de vCenter Server del clúster de confianza mediante vSphere Client.

2 Inicie sesión como administrador.

   Puede iniciar sesión como administrador de Trust Authority o administrador de vSphere.

3 Desplácese hasta un centro de datos y haga clic en la pestaña **Supervisar**.

4 Haga clic en **Seguridad**.

5 Revise el estado del host de confianza en la columna Atestación y lea el mensaje adjunto en la columna Mensaje.

Pasos siguientes

Si se producen errores, consulte Solucionar problemas de atestación de host de confianza.

Solucionar problemas de atestación de host de confianza

Los informes de atestación de vSphere Trust Authority ofrecen un punto de partida para solucionar los errores de atestación de host de confianza.

Procedimiento

1 Ver el estado de atestación de un clúster de confianza.

2 Utilice la siguiente tabla para solucionar los problemas y resolver los errores.

Error	Causa y solución
Servicios de atestación no configurados.	No se configuraron los servicios de atestación. Configure el host de confianza para que use los servicios de atestación mediante la acción Corregir. Consulte Corregir un clúster de confianza.
No hay ningún dispositivo con TPM2 disponible.	Instale y configure el host de confianza para que use un módulo de plataforma de confianza (Trusted Platform Module, TPM). Consulte la documentación del proveedor.
No se pudieron recuperar el certificado o la clave pública de aprobación de TPM2.	Compruebe que el TPM sea compatible y que tenga una clave de aprobación válida. Es posible que deba ponerse en contacto con el soporte de VMware.
El informe de atestación no está disponible.	Es posible que el host de confianza no haya finalizado la atestación. Espere unos minutos y vuelva a comprobar el estado de la atestación.
La versión del servicio de atestación no es compatible con la solicitud.	Actualice el host de Trust Authority que ejecuta el servicio de atestación para vSphere 7.0 Update 1 o una versión posterior.
Se produjo un error en la atestación porque el arranque seguro no está habilitado.	Compruebe que el host de confianza esté configurado para usar el arranque seguro. Consulte Arranque seguro UEFI para hosts ESXi.
La atestación no pudo identificar la versión de software remoto.	Importe la información de la imagen base del host de confianza en el servicio de atestación. Consulte Importar la información del host de confianza en el clúster de Trust Authority.
Se produjo un error en la atestación porque se requiere un certificado de TPM.	Compruebe que el TPM sea compatible. De forma alternativa, ejecute el siguiente cmdlet de PowerCLI para modificar com.vmware.esx.attestation.tpm2.settings para establecer en `requireCertificateValidation` en `false`. `Set-TrustAuthorityTpm2AttestationSettings` `-TrustAuthorityCluster` *`TrustedCluster`* `-RequireCertificateValidation:$false` `-RequireEndorsementKey:$true`

Error	Causa y solución
Se produjo un error en la atestación debido a un TPM desconocido.	Importe la clave de aprobación de TPM en los servicios de atestación. Consulte Importar la información del host de confianza en el clúster de Trust Authority.
Error: vapi.send.failed.	Es posible que el servicio kmxa no se esté ejecutando en el host de confianza o que el servicio kmxa no se pueda poner en contacto con el servicio de atestación. Asegúrese de que se haya iniciado el servicio kmxa. Además, compruebe que se esté ejecutando el servicio de atestación. Consulte Reiniciar el servicio de host de confianza.

Comprobar y corregir el estado del clúster de confianza

El estado de un clúster de confianza se puede comprobar y validar. Si la configuración de un clúster de confianza no está en buen estado, debe resolver las inconsistencias de la configuración. Para ello, se corrige el clúster de confianza. Al corregir un clúster de confianza, se asegura de que todos los hosts de confianza del clúster de confianza tengan la misma configuración de confianza.

Un clúster de confianza consiste en un clúster de vCenter Server de hosts ESXi de confianza que el clúster de Trust Authority atesta de forma remota. Al configurar vSphere Trust Authority inicialmente, debe importar la información de los servicios de Trust Authority del clúster de Trust Authority en el clúster de confianza. El clúster de confianza utiliza esa configuración de componentes para ponerse en contacto con el servicio de proveedor de claves y el servicio de atestación que se ejecutan en el clúster de Trust Authority. Para obtener más información sobre este aspecto de la configuración del clúster de confianza, consulte Importar la información del clúster de Trust Authority en los hosts de confianza. Después de configurar un clúster de confianza, puede comprobar y corregir su estado.

Comprobar el estado del clúster de confianza

La comprobación del estado de un clúster de confianza depende de lo siguiente.

Configuración de estado deseado

La configuración de estado deseado se basa en la información de los servicios de Trust Authority que se importa en el clúster de confianza. La configuración de estado deseado es la "fuente de la verdad" del clúster de confianza. Piense en la configuración de estado deseado como la que se crea inicialmente al configurar el clúster de confianza.

Configuración aplicada

La configuración aplicada es el registro de los servicios de atestación específicos y los servicios de proveedor de claves para los que se configuró el clúster de confianza. La configuración aplicada es la forma en la que el clúster de confianza se está ejecutando en este momento. Puede pensar en la configuración aplicada como la configuración de "tiempo de ejecución". La configuración de estado deseado debe coincidir con la configuración aplicada. Sin embargo, si la configuración aplicada no es coherente con la configuración de estado deseado, se considera que el clúster de confianza "no está en buen estado". Un

clúster de confianza que no está en buen estado puede experimentar un menor rendimiento o puede que no funcione en absoluto.

Esta comprobación de estado no es un indicador del estado general de un clúster de confianza ni de la infraestructura de vSphere Trust Authority. La comprobación de estado solo compara la configuración de estado deseado del clúster de confianza con la configuración aplicada.

Corregir el clúster de confianza

La corrección es el proceso mediante el cual vSphere Trust Authority resuelve una configuración incoherente de un clúster de confianza. La configuración de un clúster de confianza puede volverse incoherente a lo largo del tiempo o debido a otros errores operativos.

Utilice la corrección de la siguiente manera:

- Compruebe el estado del clúster de confianza.
- Si el clúster de confianza tiene un estado incorrecto, corríjalo.

Puede utilizar vSphere Client o la CLI para comprobar el estado del clúster de confianza. Consulte Comprobar el estado del clúster de confianza. También puede utilizar vSphere Client o la CLI para corregir un clúster de confianza. Consulte Corregir un clúster de confianza.

Nota La corrección también es el proceso apropiado para usar cuando se agrega un host a un clúster de confianza existente. Consulte Agregar un host a un clúster de confianza mediante vSphere Client y Agregar un host a un clúster de confianza mediante la línea de comandos.

Comprobar el estado del clúster de confianza

Puede comprobar el estado de un clúster de confianza mediante vSphere Client o la línea de comandos.

Requisitos previos

- La instancia de vCenter Server para el clúster de confianza debe ejecutar vSphere 7.0 Update 1 o versiones posteriores.
- Si utiliza PowerCLI, se requiere la versión 12.1.0 o una versión posterior.

Procedimiento

1 Compruebe el estado del clúster de confianza.

Herramienta	Pasos
vSphere Client	a Conéctese a la instancia de vCenter Server del clúster de confianza mediante vSphere Client. b Inicie sesión como administrador de Trust Authority. c Vaya a un clúster de confianza, seleccione **Configurar** y, a continuación, seleccione **Trust Authority**. d Haga clic en **Comprobar estado**.
CLI	a En una sesión de PowerCLI, ejecute el cmdlet `Connect-VIServer` para conectarse como administrador de Trust Authority a la instancia de vCenter Server del clúster de confianza. `Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password 'password'` b Ejecute el cmdlet `Get-TrustedClusterAppliedStatus`, por ejemplo: `Get-TrustedClusterAppliedStatus -TrustedCluster 'TrustedCluster'`

2 Si se producen errores, consulte Corregir un clúster de confianza.

Corregir un clúster de confianza

Puede corregir la configuración de un clúster de confianza mediante vSphere Client o la línea de comandos.

Requisitos previos

La instancia de vCenter Server para el clúster de confianza debe ejecutar vSphere 7.0 Update 1 o versiones posteriores.

Procedimiento

1 Conéctese a la instancia de vCenter Server del clúster de confianza.

Herramienta	Pasos
vSphere Client	a Conéctese a la instancia de vCenter Server del clúster de confianza mediante vSphere Client. b Inicie sesión como administrador de Trust Authority.
CLI	En una sesión de PowerCLI, ejecute el cmdlet `Connect-VIServer` para conectarse como administrador de Trust Authority a la instancia de vCenter Server del clúster de confianza. `Connect-VIServer -server dirección_ip_TrustedCluster_VC -User usuario_admin_confianza -Password 'contraseña'`

2 Corrija el clúster de confianza y vuelva a comprobar su estado.

Herramienta	Pasos
vSphere Client	a Desplácese hasta un clúster de confianza. b Seleccione **Configurar** y, a continuación, seleccione **Trust Authority**. c Haga clic en **Corregir**. d Haga clic en **Comprobar estado**.
CLI	a Ejecute el cmdlet `Set-TrustedCluster` con el parámetro `-Remediate`, por ejemplo: `Set-TrustedCluster -TrustedCluster 'TrustedCluster' -Remediate` b Ejecute el cmdlet `Get-TrustedClusterAppliedStatus`, por ejemplo: `Get-TrustedClusterAppliedStatus -TrustedCluster 'TrustedCluster'`

Usar el cifrado en el entorno de vSphere

10

Si utiliza un proveedor de claves estándar, uno de confianza, o vSphere Native Key Provider, el uso de cifrado en el entorno de vSphere requiere algo de preparación.

Consulte la siguiente información para configurar el entorno de forma que use un proveedor de claves:

- Capítulo 7 Configurar y administrar un proveedor de claves estándar
- Capítulo 8 Configurar y administrar el proveedor de claves nativo de vSphere
- Configurar vSphere Trust Authority

Una vez que el entorno está configurado, se puede usar vSphere Client para crear máquinas virtuales y discos virtuales cifrados, así como cifrar discos y máquinas virtuales existentes.

Se pueden usar la API y la CLI de `crypto-util` para realizar tareas adicionales. Consulte la *Guía de programación de vSphere Web Services SDK* para ver la documentación de API y la ayuda de la línea de comandos `crypto-util` para ver detalles de esa herramienta.

Lea los siguientes temas a continuación:

- Crear una directiva de almacenamiento de cifrado
- Activar el modo de cifrado de host de forma explícita
- Desactivar el modo de cifrado de host mediante la API
- Crear una máquina virtual cifrada
- Clonar una máquina virtual cifrada
- Cifrar una máquina virtual o un disco virtual existente
- Descifrar una máquina virtual o un disco virtual cifrados
- Cambiar la directiva de cifrado para discos virtuales
- Resolver problemas de claves de cifrado que faltan
- Desbloquear las máquinas virtuales bloqueadas
- Solucionar problemas del modo de cifrado de host ESXi
- Volver a activar el modo de cifrado del host ESXi
- Establecer el umbral de caducidad del certificado del servidor de claves

- Cifrado de máquinas virtuales de vSphere y volcados de núcleo
- Activar y desactivar la persistencia de claves en un host ESXi
- Cambiar la clave de una máquina virtual cifrada mediante vSphere Client
- Regenerar claves de una máquina virtual cifrada mediante la CLI
- Establecer el proveedor de claves predeterminado mediante vSphere Client
- Establecer el proveedor de claves predeterminado mediante la línea de comandos

Crear una directiva de almacenamiento de cifrado

Antes de crear máquinas virtuales cifradas, debe crear una directiva de almacenamiento de cifrado. Puede crear la directiva de almacenamiento una vez y asignarla cada vez que cifre una máquina virtual o un disco virtual.

Si desea usar el cifrado de máquinas virtuales con otros filtros de E/S, o utilizar el asistente **Crear directiva de almacenamiento de máquina virtual** en vSphere Client, consulte la documentación *Almacenamiento de vSphere* para obtener detalles.

Requisitos previos

- Configure la conexión con un proveedor de claves.

  Si bien puede crear una directiva de almacenamiento de cifrado de máquinas virtuales sin conectarse al proveedor de claves, no es posible realizar tareas de cifrado hasta que se haya establecido una conexión de confianza con el proveedor de claves.
- Privilegios necesarios: **Operaciones criptográficas.Administrar directivas de cifrado**.

Procedimiento

1. Inicie sesión en vCenter Server mediante vSphere Client.
2. Seleccione **Inicio**, haga clic en **Directivas y perfiles** y, a continuación, en **Directivas de almacenamiento de VM**.
3. Haga clic en **Crear**.
4. Seleccione la instancia de vCenter Server, introduzca un nombre de directiva, escriba una descripción de forma opcional y, a continuación, haga clic en **Siguiente**.
5. En la página **Estructura de directiva**, compruebe **Habilitar funciones basadas en host** y, a continuación, haga clic en **Siguiente**.
6. En la página **Servicios basados en hosts**, seleccione **Usar componente de directiva de almacenamiento**, elija **Propiedades de cifrado predeterminadas** en el menú desplegable y, a continuación, haga clic en **Siguiente**.
7. En la página **Compatibilidad de almacenamiento**, deje seleccionada la opción **Compatible**, elija un almacén de datos y, a continuación, haga clic en **Siguiente**.
8. Revise la información y haga clic en **Finalizar**.

Resultados

La directiva de almacenamiento de cifrado de máquinas virtuales se agrega a la lista y está disponible para su uso al cifrar una máquina virtual.

Activar el modo de cifrado de host de forma explícita

Es necesario establecer el modo de cifrado de host cuando se desea ejecutar tareas de cifrado, como crear una máquina virtual cifrada, en un host ESXi. En la mayoría de los casos, el modo de cifrado de host se activa automáticamente cuando se realiza una tarea de cifrado.

En ocasiones, es necesario activar el modo de cifrado de forma explícita. Consulte Requisitos previos y privilegios necesarios para tareas de cifrado de máquinas virtuales.

Requisitos previos

Privilegio necesario: **Operaciones criptográficas. Registrar host**

Procedimiento

1 Inicie sesión en vCenter Server mediante vSphere Client.

2 Desplácese hasta el host ESXi y haga clic en **Configurar**.

3 En Sistema, haga clic en **Perfil de seguridad**.

4 Haga clic en **Editar** en el panel Modo de cifrado de host.

5 Seleccione **Habilitado** y haga clic en **Aceptar**.

Desactivar el modo de cifrado de host mediante la API

El modo de cifrado de host se activa automáticamente cuando un usuario realiza una tarea de cifrado si el usuario tiene privilegios suficientes. Una vez activado el modo de cifrado de host, se cifran todos los volcados de núcleos para evitar la divulgación de información confidencial entre el personal de soporte. Si ya no se usa el cifrado de máquinas virtuales con un host ESXi, se puede desactivar el modo de cifrado.

Después de activar el modo de cifrado para un host ESXi, es posible que tenga que desactivarlo. Por ejemplo, es posible que tenga que desactivar el modo de cifrado para generar un paquete de soporte de ESXi (mediante el comando `vm-support`). Utilizar el conmutador del modo de cifrado de host (**Host > Configurar > Perfil de seguridad > Editar modo de cifrado de host**) no funciona cuando existe material de clave en el host.

Puede utilizar la API para desactivar el modo de cifrado de host si invoca el método de API `CryptoManagerHostDisable`.

Los modos de cifrado, o los estados, definidos para un host ESXi son los siguientes:

- pendingIncapable: el host está desactivado para el cifrado; es decir, el host no puede realizar operaciones de cifrado de máquinas virtuales de vSphere.

- incapaz (incapable): el host no es seguro para recibir material confidencial.
- preparado (prepared): el host está preparado para recibir material confidencial, pero aún no tiene una clave de host configurada.
- seguro (safe): el host es seguro para el cifrado (activado) y tiene un conjunto de claves de host, es decir, las operaciones de cifrado de máquinas virtuales de vSphere son posibles.

Después de invocar `CryptoManagerHostDisable` en un host, el estado de cifrado del host cambia de la siguiente manera:

- Si el estado de cifrado original del host es incapaz o preparado, el estado de cifrado del host cambia a incapaz.
- Si el estado de cifrado del host original es seguro, el estado de cifrado del host cambia a pendingIncapable.
- Si el estado de cifrado del host es pendingIncapable, el estado de cifrado del host sigue como pendingIncapable.

Esta tarea muestra cómo se desactiva el modo de cifrado del host mediante el explorador de objetos administrados (Managed Object Browser, MOB) de vCenter Server. Para obtener más información sobre el uso de la API, consulte la documentación de *vSphere Web Services API* en https://developer.vmware.com/apis/968/vsphere.

Procedimiento

1 Inicie sesión en vCenter Server como administrador.

2 Elimine del registro todas las máquinas virtuales cifradas del host ESXi cuyo modo de cifrado desea desactivar.

3 Acceda al MOB en vCenter Server.

```
https://vcenter_server/mob
```

4 Invoque el método `CryptoManagerHostDisable` en un host.

   a En el nombre de contenido, haga clic en **content**.

   b En rootFolder, haga clic en **group-D1 (Datacenters)**.

   c En childEntity, haga clic en el centro de datos adecuado.

   d En hostFolder, haga clic en el host correspondiente.

   e En childEntity, haga clic en el clúster correspondiente.

   f En host, haga clic en el host adecuado.

   g En configManager, haga clic en **configManager**.

h En cryptoManager, haga clic en **CryptoManagerHost-***number*.

i Haga clic en **CryptoManagerHostDisable**.

El estado de cifrado del host cambia a pendingIncapable o incapaz, en función de su estado de cifrado original.

5 Repita el paso 4 para otros hosts en los que desee desactivar el modo de cifrado.

6 Reinicie los hosts.

Resultados

Una vez desactivado el modo de cifrado de host, no podrá realizar operaciones de cifrado, como agregar máquinas virtuales cifradas, a menos que vuelva a activar el modo de cifrado de host.

Nota Después de reiniciar un host ESXi en el que desactivó el modo de cifrado, si el estado de cifrado del host era pendingIncapable originalmente, el estado de cifrado del host seguirá siendo pendingIncapable. Para volver a activar el modo de cifrado de host, vuelva a acceder al MOB de vCenter Server e invoque el método de API `ConfigureCryptoKey`. Al volver a activar el modo de cifrado de host, utilice el identificador de clave de host original si el estado de cifrado del host es pendingIncapable.

Crear una máquina virtual cifrada

Es posible usar vSphere Client para crear máquinas virtuales cifradas.

La instancia de vSphere Client filtra por directivas de almacenamiento de cifrado de máquinas virtuales, lo que facilita la creación de máquinas virtuales cifradas.

Nota La creación de una máquina virtual cifrada demanda menos tiempo y recursos de almacenamiento que el cifrado de una máquina virtual existente. De ser posible, cifre las máquinas virtuales durante el proceso de creación.

Requisitos previos

- Configure un proveedor de claves y establézcalo como predeterminado.
- Cree una directiva de almacenamiento de cifrado o utilice la muestra que se incluye en el paquete (la directiva de cifrado de máquina virtual).
- Compruebe que la máquina virtual esté apagada.
- Compruebe que dispone de los privilegios requeridos:
  - **Operaciones de cifrado.Cifrar nuevo**
  - Si el modo de cifrado del host no está habilitado, también necesita **Operaciones de cifrado.Registrar host**.

Procedimiento

1 Conéctese a vCenter Server mediante vSphere Client.

2 Seleccione un objeto del inventario que sea un objeto primario válido de una máquina virtual, por ejemplo, un host o clúster ESXi.

3 Haga clic con el botón secundario en el objeto y seleccione **Nueva máquina virtual**.

4 Siga las indicaciones para crear una máquina virtual cifrada.

Opción	Acción
Seleccionar un tipo de creación	Cree una máquina virtual nueva.
Seleccionar un nombre y una carpeta	Especifique un nombre único y una ubicación de destino para la máquina virtual.
Seleccionar un recurso informático	Especifique el objeto sobre el que tiene privilegios para crear máquinas virtuales cifradas. Consulte Requisitos previos y privilegios necesarios para tareas de cifrado de máquinas virtuales.
Seleccionar almacenamiento	Seleccione la casilla **Cifrar esta máquina virtual**. Aparecen directivas de almacenamiento de máquina virtual que incluyen cifrado. Seleccione una directiva de almacenamiento de máquina virtual (la muestra en el paquete es Directiva de cifrado de máquina virtual) y seleccione un almacén de datos compatible.
Seleccionar compatibilidad	Seleccione la compatibilidad. Una máquina virtual cifrada solo se puede migrar a hosts compatibles con ESXi 6.5 y versiones posteriores.
Seleccionar un sistema operativo invitado	Seleccione el sistema operativo invitado donde planea instalar la máquina virtual posteriormente.
Personalizar hardware	Personalice el hardware, por ejemplo, cambiando el tamaño de disco o CPU. (Opcional) Seleccione la pestaña **Opciones de máquina virtual** y expanda **Cifrado**. Seleccione los discos que desea excluir del cifrado. Cuando se anula la selección de un disco, solo se cifran el inicio de la máquina virtual y los otros discos seleccionados. Se cifra todo disco duro nuevo que se haya agregado. Se puede cambiar la directiva de almacenamiento para discos duros individuales más tarde.
Listo para finalizar	Revise la información y haga clic en **Finalizar**.

Clonar una máquina virtual cifrada

Una máquina virtual cifrada y clonada utiliza las mismas claves para cifrarse a menos que las cambie. Para cambiar las claves, puede utilizar vSphere Client, PowerCLI o la API. Si utiliza PowerCLI o la API, puede clonar la máquina virtual cifrada y cambiar las claves en un paso.

Puede realizar las siguientes operaciones durante la clonación.

- Crear una máquina virtual cifrada a partir de una máquina virtual o una plantilla de máquina virtual sin cifrar.
- Crear una máquina virtual descifrada a partir de una máquina virtual o una plantilla de máquina virtual cifrada.
- Volver a cifrar la máquina virtual de destino con claves diferentes a las de la máquina virtual de origen.

- En vSphere 8.0 y versiones posteriores, al seleccionar la opción **Reemplazar** para una máquina virtual con un vTPM, se inicia con un nuevo vTPM en blanco, que obtiene sus propios secretos e identidad.

Nota vSphere 8.0 y versiones posteriores incluyen el ajuste avanzado `vpxd.clone.tpmProvisionPolicy` para que el comportamiento de clonación predeterminado de los vTPM sea "reemplazar".

Puede crear una máquina virtual de clon instantáneo a partir de una máquina virtual cifrada, con la precaución de que el clon instantáneo comparta la misma clave con la máquina virtual de origen. No se pueden volver a cifrar claves en la máquina virtual de origen o de clon instantáneo.

Para usar la API para clonar máquinas cifradas, consulte *Guía de programación de vSphere Web Services SDK*.

Requisitos previos

- Se debe configurar y habilitar un proveedor de claves.
- Cree una directiva de almacenamiento de cifrado o utilice la muestra que se incluye en el paquete (la directiva de cifrado de máquina virtual).
- Privilegios necesarios (se aplica a todos los proveedores de claves):
  - **Operaciones criptográficas.Clonar**
  - **Operaciones criptográficas.Cifrar**
  - **Operaciones criptográficas.Descifrar**
  - **Operaciones criptográficas.Volver a cifrar**
  - Si el modo de cifrado del host no está habilitado, además debe tener privilegios de **Operaciones de cifrado.Registrar host**.

Procedimiento

1 Desplácese hasta la máquina virtual en el inventario de vSphere Client.

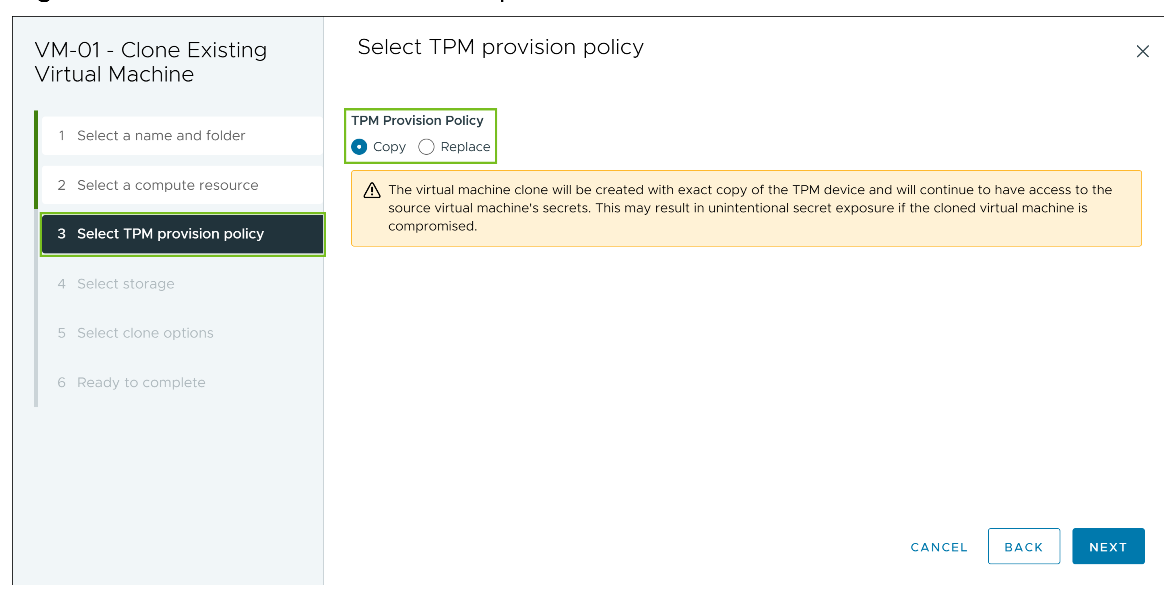
2 Para crear un clon de una máquina cifrada, haga clic con el botón derecho en la máquina virtual, seleccione **Clonar > Clonar a máquina virtual** y siga las indicaciones.

   a En la página **Seleccionar un nombre y una carpeta**, introduzca un nombre y una ubicación de destino para el clon.

   b En la página **Seleccionar un recurso informático**, especifique un objeto para el que tenga privilegios.

c (opcional) Cambie las claves del vTPM clonado.

Figura 10-1. Seleccionar directiva de aprovisionamiento de TPM



La clonación de una máquina virtual duplica la máquina virtual completa, incluidos el vTPM y sus secretos, lo cual se puede utilizar para determinar la identidad de un sistema. Para cambiar secretos en un vTPM, seleccione **Reemplazar** en **Directiva de aprovisionamiento de TPM**.

Nota Cuando se reemplazan los secretos de un vTPM, se reemplazan todas las claves, incluidas las claves relacionadas con las cargas de trabajo. Como práctica recomendada, asegúrese de que las cargas de trabajo ya no utilicen un vTPM antes de reemplazar las claves. De lo contrario, es posible que las cargas de trabajo de la máquina virtual clonada no funcionen correctamente.

d En la página **Seleccionar almacenamiento**, seleccione un almacén de datos. Se puede cambiar la directiva de almacenamiento como parte de la operación de clonación. Por ejemplo, si en lugar de utilizar una directiva de cifrado se emplea una que no es de cifrado, se descifran los discos.

e En la página **Seleccionar opciones de clonación**, seleccione las opciones de clonación, como se describe en la documentación de *Administrar máquinas virtuales de vSphere*.

f En la página **Listo para completar**, revise la información y haga clic en **Finalizar**.

3 (opcional) Cambie las claves de la máquina virtual clonada.

De forma predeterminada, la máquina virtual clonada se crea con las mismas claves que la máquina virtual principal. Una práctica recomendada es cambiar las claves de la máquina virtual clonada para asegurarse de que varias máquinas virtuales no tengan las mismas claves.

a Decida si se trata de una repetición de cifrado superficial o profunda.

Para usar otros DEK y KEK, repita un cifrado profundo de la máquina virtual clonada. Para usar otro KEK, repita un cifrado superficial de la máquina virtual clonada. Para realizar un repetición de cifrado profunda, debe apagar la máquina virtual. Puede realizar una operación de repetición de cifrado superficial mientras la máquina virtual esté encendida y si esta contiene instantáneas. La repetición de cifrado superficial de una máquina virtual cifrada con instantáneas solo se permite en una única rama de instantáneas (cadena de discos). No se admiten varias ramas de instantáneas. Si se produce un error en la repetición de cifrado superficial antes de actualizar todos los vínculos de la cadena con la nueva KEK, aún se puede acceder a la máquina virtual cifrada si tiene la KEK antigua y la nueva.

b Repita el cifrado del clon mediante la API. Consulte *Guía de programación de vSphere Web Services SDK*.

Cifrar una máquina virtual o un disco virtual existente

Es posible cifrar una máquina virtual o un disco virtual existente si se cambia su directiva de almacenamiento. Solo se pueden cifrar discos virtuales de máquinas virtuales cifradas.

Requisitos previos

- Configure un proveedor de claves y establézcalo como predeterminado.
- Cree una directiva de almacenamiento de cifrado o utilice la muestra que se incluye en el paquete (la directiva de cifrado de máquina virtual).
- Compruebe que la máquina virtual esté apagada.
- Compruebe que dispone de los privilegios requeridos:
  - **Operaciones de cifrado.Cifrar nuevo**
  - Si el modo de cifrado del host no está habilitado, también necesita **Operaciones de cifrado.Registrar host**.

Procedimiento

1 Conéctese a vCenter Server mediante vSphere Client.

2 Haga clic con el botón derecho en la máquina virtual que desea modificar y seleccione **Directivas de máquina virtual > Editar directivas de almacenamiento de máquina virtual**.

   Es posible establecer la directiva de almacenamiento para los archivos de la máquina virtual, que se representan con Inicio de la máquina virtual, y la directiva de almacenamiento para los discos virtuales.

3 Seleccione la directiva de almacenamiento.

   - Para cifrar la máquina virtual y sus discos duros, seleccione una directiva de almacenamiento de cifrado y haga clic en **Aceptar**.
   - Para cifrar la máquina virtual, pero no los discos virtuales, active **Configurar por disco**, seleccione la directiva de almacenamiento de cifrado para Inicio de la máquina virtual y otras directivas de almacenamiento para los discos virtuales, y haga clic en **Aceptar**.

   No puede cifrar el disco virtual de una máquina virtual no cifrada. Sin embargo, si utiliza vSphere Client para cifrar los archivos de inicio de la máquina virtual, puede volver a configurarla sin cifrar con el disco cifrado.

4 Si lo prefiere, puede cifrar la máquina virtual, o la máquina virtual y los discos, en el menú **Editar configuración** de vSphere Client.

   a Haga clic con el botón derecho en la máquina virtual y seleccione **Editar configuración**.

   b Seleccione la pestaña **Opciones de máquina virtual** y abra **Cifrado**. Elija una directiva de cifrado. Si anula la selección de todos los discos, solo se cifrará el inicio de la máquina virtual.

   c Haga clic en **Aceptar**.

Descifrar una máquina virtual o un disco virtual cifrados

Puede descifrar una máquina virtual, sus discos o ambos si cambia la directiva de almacenamiento.

Esta tarea describe cómo descifrar una máquina virtual cifrada mediante vSphere Client.

Todas las máquinas virtuales cifradas requieren vMotion cifrado. Durante el descifrado de la máquina virtual, se conserva la configuración de vMotion cifrado. Para cambiar esta opción y dejar de usar vMotion cifrado, cambie de forma explícita la configuración.

En esta tarea se explica la forma de ejecutar el descifrado mediante las directivas de almacenamiento. En los discos virtuales, se puede realizar el descifrado mediante el menú **Editar configuración**.

Nota En el panel Detalles de la máquina virtual, una máquina virtual habilitada para vTPM muestra un icono de candado y un mensaje "Cifrado con *key_provider*". Para quitar un vTPM de una máquina virtual, consulte Quitar el módulo de plataforma de confianza virtual de una máquina virtual.

Requisitos previos

- La máquina virtual debe estar cifrada.
- La máquina virtual debe estar apagada o en modo de mantenimiento.
- Privilegios necesarios: **Operaciones criptográficas.Descifrar**

Procedimiento

1 Conéctese a vCenter Server mediante vSphere Client.

2 Haga clic con el botón derecho en la máquina virtual que desea modificar y seleccione **Directivas de máquina virtual > Editar directivas de almacenamiento de máquina virtual**.

   Es posible establecer la directiva de almacenamiento para los archivos de la máquina virtual, que se representan con Inicio de la máquina virtual, y la directiva de almacenamiento para los discos virtuales.

3 Seleccione una directiva de almacenamiento.

   - Para descifrar la máquina virtual y sus discos duros, desactive **Configurar por disco**, seleccione una directiva de almacenamiento en el menú desplegable y haga clic en **Aceptar**.
   - Para descifrar un disco virtual, pero no la máquina virtual, active **Configurar por disco**, seleccione la directiva de almacenamiento de cifrado para Inicio de la máquina virtual y otras directivas de almacenamiento correspondientes a los discos virtuales, y haga clic en **Aceptar**.

   No se puede descifrar la máquina virtual y dejar el disco cifrado.

4 Si lo prefiere, puede usar vSphere Client para descifrar la máquina virtual y los discos en el menú **Editar configuración**.

   a Haga clic con el botón derecho en la máquina virtual y seleccione **Editar configuración**.

   b Seleccione la pestaña **Opciones de máquina virtual** y expanda **Cifrado**.

   c Para descifrar la máquina virtual y sus discos duros, elija **Ninguno** en el menú desplegable **Cifrar máquina virtual**.

   d Para descifrar un disco virtual, pero no la máquina virtual, anule la selección del disco.

   e Haga clic en **Aceptar**.

5 (opcional) Puede modificar la opción de configuración vMotion cifrado.

   a Haga clic con el botón derecho en la máquina virtual y, a continuación, haga clic en **Editar configuración**.

   b Haga clic en **Opciones de máquina virtual** y abra **Cifrado**.

   c Establezca el valor de **vMotion cifrado**.

Cambiar la directiva de cifrado para discos virtuales

Cuando crea una máquina virtual cifrada desde vSphere Client, puede elegir cuáles de los discos virtuales que se agregan durante la creación de la máquina virtual se cifran. Puede descifrar discos virtuales que están cifrados con la opción **Editar directivas de almacenamiento de máquina virtual**.

Nota Una máquina virtual cifrada puede tener discos virtuales que no estén cifrados. Sin embargo, una máquina virtual no cifrada no puede tener discos virtuales cifrados.

Consulte Cifrado de disco virtual.

En esta tarea, se describe la forma de cambiar la directiva de cifrado mediante directivas de almacenamiento. También puede usar el menú **Editar configuración** para realizar este cambio.

Requisitos previos

- Debe tener el privilegio **Operaciones criptográficas.Administrar directivas de cifrado**.
- Compruebe que la máquina virtual esté apagada.

Procedimiento

1 Conéctese a vCenter Server mediante vSphere Client.

2 Haga clic con el botón derecho en la máquina virtual y seleccione **Directivas de máquina virtual > Editar directivas de almacenamiento de máquina virtual**.

3 Cambie la directiva de almacenamiento.

   - Para cambiar la directiva de almacenamiento de la máquina virtual y sus discos duros, seleccione una directiva de almacenamiento de cifrado y haga clic en **Aceptar**.
   - Para cifrar la máquina virtual, pero no los discos virtuales, active **Configurar por disco**, seleccione la directiva de almacenamiento de cifrado para Inicio de la máquina virtual y otras directivas de almacenamiento para los discos virtuales, y haga clic en **Aceptar**.

   No se puede cifrar el disco virtual de una máquina virtual sin cifrar.

4 Si lo prefiere, puede cambiar la directiva de almacenamiento desde el menú **Editar configuración**.

   a Haga clic con el botón derecho en la máquina virtual y seleccione **Editar configuración**.

   b Seleccione la pestaña **Hardware virtual**, expanda un disco duro y seleccione una directiva de cifrado en el menú desplegable.

   c Haga clic en **Aceptar**.

Resolver problemas de claves de cifrado que faltan

Si el host ESXi no puede obtener la clave (KEK) de vCenter Server para una máquina virtual cifrada o un disco virtual cifrado, la máquina virtual cifrada se bloquea. Después de hacer que las

claves estén disponibles en el servidor de claves (KMS), puede desbloquear una máquina virtual cifrada bloqueada.

En ciertas circunstancias, cuando se utiliza un proveedor de claves estándar, el host ESXi no puede obtener la clave de cifrado de claves (KEK) para una máquina virtual cifrada o un disco virtual cifrado desde vCenter Server. En ese caso, todavía puede cancelar el registro o volver a cargar la máquina virtual. Sin embargo, no puede realizar otras operaciones con la máquina virtual, como encenderla. Después de realizar los pasos necesarios para que las claves requeridas estén disponibles en el servidor de claves, puede desbloquear una máquina virtual cifrada bloqueada mediante vSphere Client.

Si la clave de la máquina virtual no está disponible, una alarmavCenter Server le notifica y el estado de la máquina virtual se muestra como no válido. No se puede encender la máquina virtual. Si la clave de la máquina virtual está disponible, pero no hay disponible una clave para un disco cifrado, el estado de la máquina virtual no se muestra como no válido. Sin embargo, la máquina virtual no se puede encender y aparece el siguiente error:

```
The disk [/path/to/the/disk.vmdk] is encrypted and a required key was not found.
```

Nota El siguiente procedimiento muestra las situaciones que pueden causar el bloqueo de una máquina virtual, las alarmas y los registros de eventos correspondientes que aparecen y lo que se debe hacer en cada caso.

Procedimiento

1 Si el problema radica en la conexión entre el sistema vCenter Server y el servidor de claves, vCenter Server genera una alarma de máquina virtual. Además, aparece un mensaje de error en el registro de eventos.

   Restaure la conexión con el servidor de claves. Cuando el servidor de claves y las claves vuelvan a estar disponibles, desbloquee las máquinas virtuales bloqueadas. Consulte Desbloquear las máquinas virtuales bloqueadas. También puede reiniciar el host y volver a registrar la máquina virtual para desbloquearla después de restaurar la conexión.

   Al perder la conexión con el servidor de claves, no se bloquea automáticamente la máquina virtual. La máquina virtual solo entra en un estado bloqueado si se cumplen las siguientes condiciones:

   - La clave no está disponible en el host ESXi.
   - vCenter Server no puede recuperar claves del servidor de claves.

   Después de cada reinicio de ESXi, es deseable, aunque no necesario, que vCenter Server se inicie primero. vCenter Server solicita la clave con el identificador correspondiente del servidor de claves y la pone a disposición de ESXi.

   Nota En vSphere 7.0 Update 2 y versiones posteriores, puede conservar las claves de cifrado en ESXi reinicios. Consulte Persistencia de claves de vSphere en hosts ESXi.

Si la máquina virtual permanece bloqueada después de restaurar la conexión con el proveedor de claves, consulte Desbloquear las máquinas virtuales bloqueadas.

2 Si se restaura la conexión, registre la máquina virtual. Si se produce un error o si la operación se realiza correctamente, pero la máquina virtual está en estado bloqueado, compruebe que tiene el privilegio **Operaciones criptográficas.Registro de máquina virtual** para el sistema vCenter Server.

   Este privilegio no es necesario para encender una máquina virtual cifrada si la clave está disponible. No obstante, sí es necesario para registrar la máquina virtual si la clave debe recuperarse.

3 Si la clave ya no está disponible en el servidor de claves, vCenter Server genera una alarma de máquina virtual. Además, aparece un mensaje de error en el registro de eventos.

   Solicite al administrador del servidor de claves que restaure la clave. Puede encontrar una clave inactiva si va a encender una máquina virtual que se había quitado del inventario y no se había registrado por un largo período. También sucede si reinicia el host ESXi y el servidor de claves no está disponible.

   a Recupere el identificador de clave mediante el explorador de objetos administrados (Managed Object Browser, MOB) o vSphere API.

      Recupere el valor de `keyId` de `VirtualMachine.config.keyId.keyId`.

   b Solicite al administrador del servidor de claves que reactive la clave que está asociada con ese identificador de clave.

   c Tras restaurar la clave, consulte Desbloquear las máquinas virtuales bloqueadas.

   Si la clave se puede restaurar en el servidor de claves, vCenter Server la recupera y la envía al host ESXi la próxima vez que la necesite.

4 Si se puede acceder al servidor de claves y el host ESXi está encendido, pero el sistema vCenter Server no está disponible, siga estos pasos para desbloquear las máquinas virtuales.

   a Restaure el sistema vCenter Server o configure un sistema vCenter Server diferente y, a continuación, establezca confianza con el servidor de claves.

      Debe usar el mismo nombre del proveedor de claves, pero la dirección IP del servidor de claves puede ser diferente.

   b Vuelva a registrar todas las máquinas virtuales que están bloqueadas.

      La nueva instancia de vCenter Server recupera las claves del servidor de claves y las máquinas virtuales se desbloquean.

5 Si faltan las claves solo en el host ESXi, vCenter Servergenera una alarma de máquina virtual y aparece el siguiente mensaje en el registro de eventos:

   `La máquina virtual está bloqueada porque faltan claves en el host.`

   El sistema vCenter Server puede recuperar las claves que faltan desde el proveedor de claves. No se requiere la recuperación manual de las claves. Consulte Desbloquear las máquinas virtuales bloqueadas.

Desbloquear las máquinas virtuales bloqueadas

Una alarma de vCenter Server notifica cuando una máquina virtual cifrada se encuentra en estado bloqueado. Para desbloquear una máquina virtual cifrada bloqueada, puede usar vSphere Client después de realizar los pasos necesarios a fin de que las claves requeridas estén disponibles en el servidor de claves.

Requisitos previos

- Compruebe que cuenta con los privilegios necesarios: **Operaciones criptográficas.RegisterVM**.
- Podrían ser necesarios otros privilegios para realizar tareas opcionales, como habilitar el cifrado de host.
- Antes de desbloquear una máquina virtual bloqueada, resuelva la causa del bloqueo e intente solucionar el problema manualmente. Consulte Resolver problemas de claves de cifrado que faltan.

Procedimiento

1 Conéctese a vCenter Server mediante vSphere Client.

2 Desplácese hasta la pestaña **Resumen** de la máquina virtual.

   Cuando una máquina virtual está bloqueada, aparece la alarma de máquina virtual bloqueada.

3 Decida si quiere confirmar la alarma o restablecerla en verde, pero sin desbloquear ahora la máquina virtual.

   Al hacer clic en **Confirmar** o **Restablecer a verde**, la alarma desaparece, pero la máquina virtual permanecerá bloqueada hasta que la desbloquee.

4 Desplácese hasta la pestaña **Supervisar** de la máquina virtual y haga clic en **Eventos**.

   El panel **Eventos** muestra información sobre el motivo por el que la máquina virtual está bloqueada.

5 Antes de desbloquear la máquina virtual, solucione los problemas según lo sugerido.

6 Desplácese hasta la pestaña **Resumen** de la máquina virtual.

   Aparecerá una alarma de bloqueo de máquina virtual.

7 Seleccione **Desbloquear máquina virtual** en el menú desplegable **Acciones** en el lado derecho.

Solucionar problemas del modo de cifrado de host ESXi

En ciertas circunstancias, el modo de cifrado del host ESXi puede desactivarse.

Un host ESXi requiere que esté activado el modo de cifrado de ese host si contiene máquinas virtuales cifradas. Si el host detecta que falta su clave de host o si el proveedor de claves no está disponible, es posible que el host no logre activar el modo de cifrado. vCenter Server genera una alarma cuando no se puede activar el modo de cifrado del host.

Procedimiento

1 Si el problema es la conexión entre el sistema vCenter Server y el proveedor de claves, se genera una alarma y aparece el siguiente mensaje en el registro de eventos.

   Debe restaurar la conexión con el proveedor de claves que contiene las claves de cifrado en cuestión.

2 Si faltan claves, se genera una alarma y aparece un mensaje de error en el registro de eventos.

   Debe asegurarse de que las claves estén presentes en el proveedor de claves. Consulte la documentación del proveedor de administración de claves para obtener información sobre cómo restaurar a partir de una copia de seguridad.

Pasos siguientes

Si el modo de cifrado del host permanece desactivado después de restaurar la conexión con el proveedor de claves o de recuperar manualmente las claves para el proveedor de claves, vuelva a activar el modo de cifrado de host. Consulte Volver a activar el modo de cifrado del host ESXi.

Volver a activar el modo de cifrado del host ESXi

En vSphere 6.7 y versiones posteriores, una alarma de vCenter Server notifica cuándo se desactiva el modo de cifrado del host ESXi. Puede volver a activar el modo de cifrado del host si se desactivó.

Requisitos previos

- Compruebe que cuenta con los privilegios necesarios: **Operaciones criptográficas.Registrar host**.
- Antes de volver a activar el modo de cifrado, investigue la causa e intente solucionar el problema manualmente.

Procedimiento

1 Conéctese a vCenter Server mediante vSphere Client.

2 Navegue hasta la pestaña **Resumen** del host ESXi.

   Cuando se desactiva el modo de cifrado, se muestra la alarma que indica que es necesario habilitar el modo de cifrado en el host.

3 Decida si quiere confirmar la alarma o restablecerla en verde, pero sin volver a activar el modo de cifrado de host ahora.

   Al hacer clic en **Confirmar** o **Restablecer a verde**, la alarma desaparece, pero el modo de cifrado del host sigue desactivado hasta que vuelva a activarlo.

4 Desplácese hasta la pestaña **Supervisar** del host ESXi y haga clic en **Eventos**.

   Se muestra más información sobre por qué el modo de cifrado está desactivado. Solucione los problemas como se sugiere antes de volver a activar el modo de cifrado.

5 En la pestaña **Resumen**, haga clic en **Habilitar modo de cifrado de host** para volver a activar el cifrado de host.

   Se muestra un mensaje para advertir que los datos de claves de cifrado se transmitirán al host.

6 Haga clic en **Sí**.

Establecer el umbral de caducidad del certificado del servidor de claves

De forma predeterminada, vCenter Server envía una notificación 30 días antes de que caduquen los certificados del servidor de claves (KMS). Puede cambiar este valor predeterminado.

Los certificados del servidor de claves tienen una fecha de caducidad. Recibirá una alerta cuando se alcance el umbral de la fecha de caducidad.

vCenter Server y los servidores de claves intercambian dos tipos de certificados: servidor y cliente. La instancia de VMware Endpoint Certificate Store (VECS) del sistema vCenter Server almacena los certificados del servidor y un certificado de cliente por cada proveedor de claves. Debido a que existen dos tipos de certificados, hay dos alarmas para cada tipo de certificado (una para el cliente y una para el servidor).

Procedimiento

1 Inicie sesión en un sistema vCenter Server mediante vSphere Client.

2 Seleccione el sistema de vCenter Server en la jerarquía de objetos.

3 Haga clic en **Configurar**.

4 En **Configuración**, haga clic en **Configuración avanzada** y, a continuación, en **Editar configuración**.

5 Haga clic en el icono **Filtrar** e introduzca `vpxd.kmscert.threshold`, o bien desplácese hasta el propio parámetro de configuración.

6 Escriba el valor en días y haga clic en **Guardar**.

Cifrado de máquinas virtuales de vSphere y volcados de núcleo

Si el entorno utiliza cifrado de máquinas virtuales de vSphere y si se produce un error en el host ESXi, el volcado de núcleo resultante se cifra para proteger los datos del cliente. Los volcados de núcleo que se incluyen en el paquete de vm-support también están cifrados.

Nota Los volcados de núcleo pueden contener información confidencial. Siga la directiva de seguridad de datos y privacidad de la organización al gestionar el volcado de núcleo.

Volcados de núcleo en hosts ESXi

Cuando un host ESXi, el ámbito de un usuario o una máquina virtual fallan, se genera un volcado de núcleo y se reinicia el host. Si el host ESXi tiene habilitado el modo de cifrado, el volcado de núcleo se cifra con una clave que se encuentra en la memoria caché de claves de ESXi. (Según el proveedor de claves en uso, la clave proviene de un servidor de claves externo, el servicio de proveedor de claves o vCenter Server). Consulte Cómo el cifrado de máquinas virtuales de vSphere protege el entorno para obtener información general.

Cuando un host ESXi es "seguro" desde el punto de vista de cifrado y se genera un volcado de núcleo, se crea un evento. El evento indica que produjo un volcado de núcleo, junto con la siguiente información: nombre del mundo, horas en que se produjo, identificador de la clave que se utiliza para cifrar el volcado de núcleo y el nombre de archivo del volcado de núcleo. Puede ver el evento en Visor de eventos en **Tareas y eventos** para vCenter Server.

En la siguiente tabla, se muestran las claves de cifrado que se utilizan para cada tipo de volcado de núcleo, según la versión de vSphere.

Tabla 10-1. Claves de cifrado de volcado de núcleo

Tipo de volcado de núcleo	Clave de cifrado (ESXi 6.5)	Clave de cifrado (ESXi 6.7 y versiones posteriores)
Kernel de ESXi	Clave de host	Clave de host
Ámbito del usuario (hostd)	Clave de host	Clave de host
Máquina virtual cifrada	Clave de host	Clave de la máquina virtual

Las acciones que puede realizar después de un reinicio del host ESXi dependen de varios factores.

- En la mayoría de los casos, el proveedor de claves intenta insertar la clave en el host ESXi después de reiniciarlo. Si la operación se realiza correctamente, se puede generar el paquete de vm-support y descifrar el volcado de núcleo, o bien volver a cifrarlo. Consulte Descifrar o volver a cifrar un volcado de núcleo cifrado.
- Si vCenter Server no puede conectarse al host ESXi, tal vez pueda recuperar la clave. Consulte Resolver problemas de claves de cifrado que faltan.

- Si el host usó una clave personalizada que no es igual a la clave que vCenter Server inserta en el host, no podrá manipular el volcado de núcleo. Evite usar claves personalizadas.

Volcados de núcleo y paquetes de vm-support

Si se comunica con el soporte técnico de VMware debido a un error grave, el representante de soporte, por lo general, le pedirá que genere un paquete de vm-support. El paquete incluye archivos de registro y otra información, incluso volcados de núcleo. Si los representantes de soporte no pueden resolver los inconvenientes al analizar los archivos de registro y otra información, tal vez le soliciten que descifre los volcados de núcleo y que habilite la información relevante. Para proteger información confidencial, como las claves, siga la directiva de privacidad y seguridad de su organización. Consulte Recopilar un paquete de vm-support para un host ESXi que usa cifrado.

Volcados de núcleo de sistemas de vCenter Server

Un volcado de núcleo de un sistema de vCenter Server no está cifrado. vCenter Server ya contiene información posiblemente confidencial. Como mínimo, asegúrese de que vCenter Server esté protegido. Consulte Capítulo 4 Proteger sistemas vCenter Server. Asimismo, también se recomienda apagar los volcados de núcleo del sistema de vCenter Server. Otra información de los archivos de registro puede ayudar a determinar el problema.

Recopilar un paquete de vm-support para un host ESXi que usa cifrado

Si se habilita el modo de cifrado de hosts para el host ESXi, se cifran los volcados de núcleo presentes en el paquete de `vm-support`. Puede recopilar el paquete desde vSphere Client y especificar una contraseña si piensa descifrar el volcado de núcleo más adelante.

El paquete de `vm-support` incluye archivos de registro, archivos de volcado de núcleo, entre otros.

Requisitos previos

Informe a su representante de soporte si se habilita el modo de cifrado para el host ESXi. Es posible que el representante le pida descifrar los volcados de núcleo y extraer información relevante.

Nota Los volcados de núcleo pueden contener información confidencial. Siga la directiva de seguridad y privacidad de la organización para proteger información confidencial, como claves de host.

Procedimiento

1 Inicie sesión en el sistema vCenter Server mediante vSphere Client.

2 Haga clic en **Hosts y clústeres**, y haga clic con el botón secundario en el host ESXi.

3 Seleccione **Exportar registros del sistema**.

4 En el cuadro de diálogo, seleccione **Contraseña para volcados de núcleo cifrados** y, a continuación, especifique y confirme una contraseña.

5 Deje los valores predeterminados para las otras opciones o realice cambios si así lo requiere el soporte técnico de VMware, y haga clic en **Exportar registros**.

   Si no ha configurado el navegador para preguntar dónde guardar los archivos antes de la descarga, esta se iniciará. Si efectivamente ha configurado el navegador para tal fin, especifique una ubicación para el archivo.

6 Si su representante de soporte le pidió descifrar el volcado de núcleo en el paquete de `vm-support`, inicie sesión en cualquier host ESXi y siga estos pasos.

   a Inicie sesión en el host ESXi y conéctese al directorio donde está ubicado el paquete de `vm-support`.

      El nombre de archivo sigue el patrón esx.fecha_hora.tgz.

   b Asegúrese de que el directorio tenga suficiente espacio para el paquete, el paquete descomprimido y el paquete nuevamente comprimido; o bien mueva el paquete.

   c Extraiga el paquete en el directorio local.

```
vm-support -x *.tgz .
```

      La jerarquía de archivos resultante puede contener los archivos de volcado de núcleo del host ESXi, generalmente en `/var/core`, y puede contener varios archivos de volcado de núcleo de las máquinas virtuales.

   d Descifre cada archivo de volcado de núcleo cifrado por separado.

```
crypto-util envelope extract --offset 4096 --keyfile vm-support-incident-key-file
--password encryptedZdump decryptedZdump
```

      vm-support-incident-key-file es el archivo de clave del incidente que se encuentra en el nivel superior del directorio.

      encryptedZdump es el nombre del archivo de volcado de núcleo cifrado.

      decryptedZdump es el nombre del archivo que genera el comando. Procure que el nombre sea similar al nombre de *encryptedZdump*.

   e Proporcione la contraseña que especificó al crear el paquete de `vm-support`.

   f Elimine los volcados de núcleo cifrados y vuelva a comprimir el paquete.

```
vm-support --reconstruct
```

7 Elimine los archivos que contienen información confidencial.

Descifrar o volver a cifrar un volcado de núcleo cifrado

Para descifrar o volver a cifrar un volcado de núcleo cifrado en el host ESXi, puede usar la CLI `crypto-util`.

Puede descifrar y examinar por su cuenta los volcados de núcleo en el paquete de vm-support. Los volcados de núcleo pueden contener información confidencial. Siga la directiva de seguridad y privacidad de su organización para proteger información confidencial como las claves.

Para obtener detalles sobre cómo volver a cifrar un volcado de núcleo y sobre otras funciones de `crypto-util`, consulte la ayuda de la línea de comandos.

Nota `crypto-util` es para usuarios avanzados.

Requisitos previos

La clave que se usó para cifrar el volcado de núcleo debe estar disponible en el host ESXi que generó el volcado de núcleo.

Procedimiento

1 Inicie sesión directamente en el host ESXi en donde se produjo el volcado de núcleo.

   Si el host ESXi se encuentra en el modo de bloqueo o si el acceso SSH está desactivado, es posible que deba activar el acceso en primer lugar.

2 Determine si el volcado de núcleo está cifrado.

Opción	Descripción
Supervisar el volcado de núcleo	`crypto-util envelope describe vmmcores.ve`
archivo zdump	`crypto-util envelope describe --offset 4096` *`zdumpFile`*

3 Descifre el volcado de núcleo según su tipo.

Opción	Descripción
Supervisar el volcado de núcleo	`crypto-util envelope extract vmmcores.ve vmmcores`
archivo zdump	`crypto-util envelope extract --offset 4096` *`zdumpEncrypted zdumpUnencrypted`*

Activar y desactivar la persistencia de claves en un host ESXi

Debe activar la persistencia de claves en un host ESXi. No está activada de forma predeterminada.

Para obtener información conceptual sobre la persistencia de claves, consulte Persistencia de claves de vSphere en hosts ESXi.

Requisitos previos

Requisitos para activar la persistencia de claves:

- ESXi 7.0 Update 2 o una versión posterior
- ESXi host instalado con TPM 2.0
- Tener acceso al conjunto de comandos de ESXCLI. Puede ejecutar comandos ESXCLI de forma remota o en el ESXi Shell.

Nota La persistencia de claves no es necesaria cuando se utiliza vSphere Native Key Provider. vSphere Native Key Provider está diseñado de fábrica para ejecutarse sin necesidad de acceder a un servidor de claves.

Para mayor seguridad, el TPM también puede utilizar una directiva de sellado para evitar la alteración durante el arranque del host ESXi. Consulte Qué son las directivas de sellado de TPM.

Procedimiento

1 Inicie una sesión en el host ESXi mediante SSH u otra conexión de consola remota.

2 Inicie sesión como raíz.

3 Compruebe que el host ESXi esté en modo de TPM.

```
esxcli system settings encryption get
```

Si el modo aparece como NINGUNO, debe habilitar el TPM en el firmware del host y establecer el modo mediante el siguiente comando.

```
esxcli system settings encryption set --mode=TPM
```

4 Active o desactive la persistencia de claves.

a Para activar la persistencia de claves:

```
esxcli system security keypersistence enable
```

b Para desactivar la persistencia:

```
esxcli system security keypersistence disable --remove-all-stored-keys
```

Cambiar la clave de una máquina virtual cifrada mediante vSphere Client

Puede utilizar vSphere Client para realizar una regeneración de claves superficial de una máquina virtual cifrada. Puede realizar una regeneración de claves de una máquina virtual cifrada por motivos empresariales o de cumplimiento normativo.

Una regeneración de claves superficial (también llamada "repetición de cifrado") reemplaza solo la clave de cifrado de claves (Key Encryption Key, KEK). No es necesario apagar la máquina virtual cifrada para realizar una regeneración de claves superficial. Si necesita reemplazar la clave de cifrado de disco (DEK) y la KEK, debe realizar una regeneración de claves exhaustiva.

Nota Las máquinas virtuales configuradas con controladoras IDE deben apagarse para realizar una operación de regeneración de claves superficial.

Para obtener información más detallada, consulte Cómo volver a cifrar (regenerar claves) una máquina virtual cifrada.

Requisitos previos

Privilegio necesario: **Operaciones de cifrado.Volver a cifrar**

Procedimiento

1. Inicie sesión en el sistema vCenter Server mediante vSphere Client.
2. Examine la lista de inventario y seleccione la máquina virtual cifrada.
3. Haga clic con el botón derecho en la máquina virtual cifrada y seleccione **Directivas de máquina virtual**.
4. Seleccione **Volver a cifrar**.
5. Haga clic en **Sí**.

   Se regeneran las claves de la máquina virtual cifrada con la nueva KEK.

   Nota Si se produce un error en la regeneración de claves, el subsistema de eventos publica el siguiente evento:

   ```
   com.vmware.vc.vm.crypto.RekeyFail
   ```

Regenerar claves de una máquina virtual cifrada mediante la CLI

Puede utilizar CLI para realizar una regeneración de claves superficial de una máquina virtual cifrada. Puede realizar una regeneración de claves de una máquina virtual cifrada por motivos empresariales o de cumplimiento normativo.

Una clave superficial (también llamada "repetición de cifrado") reemplaza solo la clave de cifrado de claves (Key Encryption Key, KEK). No es necesario apagar la máquina virtual cifrada para realizar una regeneración de claves superficial. Si necesita reemplazar la clave de cifrado de disco (DEK) y la KEK, debe realizar una regeneración de claves exhaustiva.

Esta tarea muestra cómo realizar una regeneración de claves superficial en una máquina virtual cifrada mediante el proveedor de claves asignado actualmente.

Para obtener información más detallada, consulte Cómo volver a cifrar (regenerar claves) una máquina virtual cifrada.

Requisitos previos

Privilegio necesario: **Operaciones de cifrado.Volver a cifrar**

Nota Las máquinas virtuales configuradas con controladoras IDE deben apagarse para realizar una operación de regeneración de claves superficial.

Procedimiento

1 En una sesión de PowerCLI, ejecute el cmdlet `Connect-VIServer` para conectarse como administrador al host de vCenter Server.

2 Asigne el proveedor de claves actual a una variable.

```
$kp = Get-KeyProvider keyprovider_name
```

3 Asigne la máquina virtual cifrada a una variable.

```
$vm = Get-VM encrypted_vm_name
```

4 Compruebe la información de seguridad de la máquina virtual cifrada.

```
Get-SecurityInfo -Entity $vm
```

Tenga en cuenta la EncryptionKeyId.

5 Realice la regeneración de claves superficial de la máquina virtual cifrada.

```
Set-VM -vm $vm -KeyProvider $kp
```

Escriba **Y** para confirmar la regeneración de claves.

6 Para comprobar que se haya cambiado EncryptionKeyId, compruebe la información de seguridad de la máquina virtual cifrada.

```
Get-SecurityInfo -Entity $vm
```

Establecer el proveedor de claves predeterminado mediante vSphere Client

Debe establecer el proveedor de claves predeterminado si no establece el primer proveedor de claves como predeterminado o si el entorno usa varios proveedores de claves y se elimina el predeterminado. Puede utilizar vSphere Client para establecer el proveedor de claves predeterminado en el nivel de vCenter Server.

Requisitos previos

Como práctica recomendada, compruebe que el estado de conexión en la pestaña Proveedores de claves sea Activo y tenga una marca de verificación verde.

Procedimiento

1 Inicie sesión en vSphere Client.

2 Desplácese hasta vCenter Server.

3 Haga clic en **Configurar** y seleccione **Proveedores de claves** en **Seguridad**.

4 Seleccione el proveedor de claves.

5 Haga clic en **Establecer como valor predeterminado**.

   Se mostrará un cuadro de diálogo de confirmación.

6 Haga clic en **Establecer como valor predeterminado**.

   El proveedor de claves se muestra como la selección predeterminada actual.

Establecer el proveedor de claves predeterminado mediante la línea de comandos

Debe establecer el proveedor de claves predeterminado si no establece el primer proveedor de claves como predeterminado o si el entorno usa varios proveedores de claves y se elimina el predeterminado. Puede usar PowerCLI para establecer el proveedor de claves predeterminado en el nivel de vCenter Server, el nivel de clúster o el nivel de carpeta del clúster.

Requisitos previos

Como práctica recomendada, compruebe que el estado de conexión en la pestaña Proveedores de claves sea Activo y tenga una marca de verificación verde.

Debe tener una función que incluya el privilegio de **Operaciones de cifrado.Administrar KMS**. En vSphere Trust Authority, la función debe aplicarse al clúster de confianza.

Procedimiento

1 Asegúrese de que está conectado como administrador a la instancia de vCenter Server donde creó el proveedor de claves.

Nota En vSphere Trust Authority, conéctese al vCenter Server del clúster de confianza.

```
Connect-VIServer -server VC_ip_address -User admin_user -Password 'password'
```

2 Obtenga el proveedor de claves.

```
Get-KeyProvider
```

Puede usar la opción `-Name` *keyprovider* para especificar un único proveedor de claves de confianza.

3 Asigne la información de proveedor de claves de confianza de `Get-KeyProvider` a una variable.

Por ejemplo, este comando asigna la información a la variable `$kp`.

```
$kp = Get-KeyProvider
```

Si cuenta con varios proveedores de claves de confianza, puede utilizar `Select-Object` para seleccionar uno de ellos.

```
$kp = Get-KeyProvider | Select-Object -Index 0
```

4 Utilice uno de los siguientes comandos de PowerCLI.

Dónde establecer el valor predeterminado	Comando
Nivel de vCenter Server	`Set-KeyProvider -KeyProvider $kp -DefaultForSystem`
Nivel de clúster	En este ejemplo, el comando establece el proveedor de claves del clúster `CL-01`. `Add-EntityDefaultKeyProvider -KeyProvider $kp -Entity 'CL-01'`
Nivel de carpeta de clúster	En este ejemplo, el comando establece el proveedor de claves de la carpeta del clúster `Cluster-Folder-01`. `Add-EntityDefaultKeyProvider -KeyProvider $kp -Entity 'Cluster-Folder-01'`

Proteger las máquinas virtuales con el módulo de plataforma de confianza virtual

11

Con la función Módulo de plataforma de confianza virtual (vTPM), puede agregar un procesador criptográfico virtual de TPM 2.0 a una máquina virtual.

Un vTPM es una representación basada en software de un chip de módulo de plataforma de confianza 2.0 físico. Un vTPM actúa como cualquier otro dispositivo virtual. Puede agregar un vTPM a una máquina virtual de la misma manera que agrega memoria, controladoras de disco, controladoras de red o CPU virtuales. Un vTPM no requiere un chip de módulo de plataforma de confianza de hardware.

Lea los siguientes temas a continuación:

Descripción de un módulo de plataforma de confianza virtual

Un módulo de plataforma de confianza virtual (virtual Trusted Platform Module, vTPM) es una representación basada en software de un chip de módulo de plataforma de confianza 2.0 físico. Un vTPM actúa como cualquier otro dispositivo virtual.

Los vTPM proporcionan funciones basadas en hardware relacionadas con la seguridad, como la generación aleatoria de números, la atestación y la generación de claves, entre otras. Cuando se agrega un vTPM a una máquina virtual, permite que el sistema operativo invitado cree y almacene claves que son privadas. Estas claves no están expuestas al sistema operativo invitado en sí. Por lo tanto, se reduce la superficie de ataque de la máquina virtual. Por lo general, al poner en peligro el sistema operativo invitado, se compromete su información confidencial, pero

la habilitación de un vTPM reduce este riesgo en gran medida. Estas claves solo las puede utilizar el sistema operativo invitado para fines de cifrado o firma. Con un vTPM asociado, un cliente puede atestar de forma remota la identidad de la máquina virtual y comprobar el software que está en ejecución.

El vTPM no requiere un chip físico de TPM 2.0 presente en el host ESXi. No obstante, si desea realizar la atestación de host, es necesaria una entidad externa, como un chip físico de TPM 2.0. Consulte Proteger hosts ESXi con el módulo de plataforma de confianza.

Nota De manera predeterminada, no hay ninguna directiva de almacenamiento asociada a una máquina virtual habilitada con un vTPM. Solo están cifrados los archivos de máquina virtual (Inicio de la máquina virtual). Si lo prefiere, puede agregar cifrado de forma explícita para la máquina virtual y sus discos, pero los archivos de máquina virtual ya se habrán cifrado.

Cómo configurar un vTPM para una máquina virtual

Desde la perspectiva de la máquina virtual, un vTPM es un dispositivo virtual. Se puede agregar un vTPM a una máquina virtual nueva o existente. Un vTPM depende del cifrado de la máquina virtual para proteger los datos esenciales de TPM; por lo que requiere que configure un proveedor de claves. Al configurar un vTPM, se cifran los archivos de la máquina virtual, pero no los discos. Puede optar por agregar cifrado de forma explícita para la máquina virtual y sus discos.

Cuando se hace una copia de seguridad de una máquina virtual habilitada con un vTPM, la copia de seguridad debe incluir todos los datos de la máquina virtual, incluido el archivo `*.nvram`. Si la copia de seguridad no incluye el archivo `*.nvram`, no se puede restaurar una máquina virtual con un vTPM. Asimismo, debido a que los archivos de inicio de una máquina virtual con un vTPM habilitado están cifrados, asegúrese de que las claves de cifrado estén disponibles en el momento de la restauración.

A partir de vSphere 8.0, al clonar una máquina virtual con un vTPM, la selección de la opción **Reemplazar** para una máquina virtual con un vTPM comienza con un vTPM nuevo y vacío, el cual obtiene sus propios secretos e identidades. Cuando se reemplazan los secretos de un vTPM, se reemplazan todas las claves, incluidas las claves relacionadas con las cargas de trabajo. Como práctica recomendada, asegúrese de que las cargas de trabajo ya no utilicen un vTPM antes de reemplazar las claves. De lo contrario, es posible que las cargas de trabajo de la máquina virtual clonada no funcionen correctamente.

Requisitos de vSphere para vTPM

Para utilizar un vTPM, el entorno de vSphere debe cumplir con estos requisitos:

- Requisitos de la máquina virtual:
  - Firmware EFI.
  - Versión de hardware 14 y posterior

- Requisitos de los componentes:
  - vCenter Server 6.7 y versiones posteriores para máquinas virtuales Windows, vCenter Server 7.0 Update 2 y versiones posteriores para máquinas virtuales Linux.
  - Cifrado de máquinas virtuales (para cifrar los archivos de inicio de la máquina virtual).
  - Proveedor de claves configurado para vCenter Server. Consulte Comparación de proveedores de claves de vSphere.
- Compatibilidad con el sistema operativo invitado:
  - Linux
  - Windows Server 2008 y versiones posteriores
  - Windows 7 y versiones posteriores

Diferencias entre un TPM de hardware y un TPM virtual

Un módulo de plataforma de confianza (Trusted Platform Module, TPM) de hardware se usa para proporcionar un almacenamiento de credenciales o claves seguro. Un vTPM realiza las mismas funciones que un TPM, pero lleva a cabo las capacidades de coprocesador cifrado en un software. El vTPM utiliza el archivo `.nvram`, que se cifra mediante el cifrado de máquinas virtuales, a modo de almacenamiento seguro.

El TPM de hardware incluye una clave precargada denominada “clave de aprobación” (Endorsement Key, EK). La EK está formada por una clave pública y una privada. La EK proporciona al TPM una identidad exclusiva. Esta clave se proporciona para un vTPM mediante VMware Certificate Authority (VMCA) o una entidad de certificación (Certificate Authority, CA) de terceros. Una vez que el vTPM utiliza una clave, por lo general, no se la cambia debido a que se invalidaría la información confidencial almacenada en el vTPM. El vTPM no se comunica con la CA externa en ningún momento.

Crear una máquina virtual con un módulo de plataforma de confianza virtual

Puede agregar un módulo de plataforma de confianza virtual (vTPM) cuando cree una máquina virtual para proporcionar mayor seguridad al sistema operativo invitado. Antes de poder agregar un vTPM, se debe crear un proveedor de claves.

El TPM virtual de VMware es compatible con TPM 2.0 y crea un chip virtual habilitado para TPM para que lo empleen la máquina virtual y el sistema operativo invitado que aloja.

Requisitos previos

- Asegúrese de que el entorno de vSphere esté configurado con un proveedor de claves. Para obtener más información, consulte la siguiente información:
  - Configurar vSphere Trust Authority
  - Capítulo 7 Configurar y administrar un proveedor de claves estándar

  - Capítulo 8 Configurar y administrar el proveedor de claves nativo de vSphere
- El sistema operativo invitado que utilice puede ser Windows Server 2008 y versiones posteriores, Windows 7 y versiones posteriores o Linux.
- Los hosts ESXi que se ejecuten en su entorno deben ser ESXi 6.7 y versiones posteriores (sistema operativo invitado Windows) o 7.0 Update 2 y versiones posteriores (sistema operativo invitado Linux).
- La máquina virtual debe usar firmware EFI.
- Compruebe que dispone de los privilegios requeridos:
  - **Operaciones de cifrado.Clonar**
  - **Operaciones de cifrado.Cifrar**
  - **Operaciones de cifrado.Cifrar nuevo**
  - **Operaciones de cifrado.Migrar**
  - **Operaciones de cifrado.Registrar máquina virtual**
  - **Operaciones de cifrado.Registrar host**

Nota Después de crear una máquina virtual con un vTPM, se requiere el privilegio **Operaciones criptográficas.Acceso directo** para abrir una sesión de consola.

Procedimiento

1 Conéctese a vCenter Server mediante vSphere Client.

2 Seleccione un objeto del inventario que sea un objeto primario válido de una máquina virtual, por ejemplo, un host o clúster ESXi.

3 Haga clic con el botón derecho en el objeto, seleccione **Nueva máquina virtual** y siga las indicaciones para crear una máquina virtual.

Opción	Acción
Seleccionar un tipo de creación	Cree una máquina virtual nueva.
Seleccionar un nombre y una carpeta	Especifique un nombre y una ubicación de destino.
Seleccionar un recurso informático	Especifique el objeto sobre el que tiene privilegios para crear máquinas virtuales. Consulte Requisitos previos y privilegios necesarios para tareas de cifrado de máquinas virtuales.
Seleccionar almacenamiento	Seleccione un almacén de datos compatible.
Seleccionar compatibilidad	Debe seleccionar **ESXi 6.7 y versiones posteriores** para el sistema operativo invitado Windows o **ESXi 7.0 U2** y versiones posteriores para el sistema operativo invitado Linux.
Seleccionar un sistema operativo invitado	Seleccione Windows o Linux para usarlo como sistema operativo invitado.

Opción	Acción
Personalizar hardware	Haga clic en **Agregar nuevo dispositivo** y seleccione **Módulo de plataforma de confianza**. Puede personalizar aún más el hardware, por ejemplo, cambiando el tamaño del disco o la CPU.
Listo para finalizar	Revise la información y haga clic en **Finalizar**.

Resultados

La máquina virtual que admite vTPM aparece en el inventario según lo especificado.

Agregar el módulo de plataforma de confianza virtual a una máquina virtual existente

Puede agregar un módulo de plataforma de confianza virtual (vTPM) a una máquina virtual existente para proporcionar una mayor seguridad al sistema operativo invitado. Antes de poder agregar un vTPM, se debe crear un proveedor de claves.

El TPM virtual de VMware es compatible con TPM 2.0 y crea un chip virtual que admite TPM para usarlo con la máquina virtual y el sistema operativo invitado que aloja.

Requisitos previos

- Asegúrese de que el entorno de vSphere esté configurado para un proveedor de claves. Para obtener más información, consulte la siguiente información:
  - Configurar vSphere Trust Authority
  - Capítulo 7 Configurar y administrar un proveedor de claves estándar
  - Capítulo 8 Configurar y administrar el proveedor de claves nativo de vSphere
- El sistema operativo invitado que utilice puede ser Windows Server 2008 y versiones posteriores, Windows 7 y versiones posteriores o Linux.
- Compruebe que la máquina virtual esté apagada.
- Los hosts ESXi que se ejecuten en su entorno deben ser ESXi 6.7 y versiones posteriores (sistema operativo invitado Windows) o 7.0 Update 2 y versiones posteriores (sistema operativo invitado Linux).
- La máquina virtual debe usar firmware EFI.
- Compruebe que dispone de los privilegios requeridos:
  - **Operaciones de cifrado.Clonar**
  - **Operaciones de cifrado.Cifrar**
  - **Operaciones de cifrado.Cifrar nuevo**
  - **Operaciones de cifrado.Migrar**

- **Operaciones de cifrado.Registrar máquina virtual**
- **Máquina virtual.Cambiar configuración.Agregar o eliminar dispositivo**

Nota Después de agregar un vTPM a una máquina virtual, se requiere el privilegio **Operaciones criptográficas.Acceso directo** para abrir una sesión de consola.

Procedimiento

1 Conéctese a vCenter Server mediante vSphere Client.

2 Haga clic con el botón derecho en la máquina virtual en el inventario que desee modificar y seleccione **Editar configuración**.

3 En el cuadro de diálogo **Editar configuración**, haga clic en **Agregar nuevo dispositivo** y seleccione **Módulo de plataforma de confianza**.

4 Haga clic en **Aceptar**.

El panel **Detalles de máquina virtual** refleja que se aplicó el cifrado a la máquina virtual.

Quitar el módulo de plataforma de confianza virtual de una máquina virtual

Puede quitar la seguridad del módulo de plataforma de confianza (vTPM) de una máquina virtual.

Si se quita un dispositivo el vTPM, la información cifrada en la máquina virtual no se podrá recuperar. Antes de quitar un vTPM de una máquina virtual, desactive todas las aplicaciones del sistema operativo invitado que utilicen el dispositivo vTPM, como BitLocker. Si no lo hace, es posible que la máquina virtual no arranque. Además, no es posible quitar un vTPM de una máquina virtual que contenga instantáneas.

Requisitos previos

- Compruebe que la máquina virtual esté apagada.
- Compruebe que dispone de los privilegios requeridos: **Máquina virtual.Cambiar configuración.Agregar o eliminar dispositivo** y **Operaciones de cifrado.Descifrar**

Procedimiento

1 Conéctese a vCenter Server mediante vSphere Client.

2 Haga clic con el botón derecho en la máquina virtual en el inventario que desee modificar y seleccione **Editar configuración**.

3 En la pestaña **Hardware virtual**, expanda **Dispositivos de seguridad**.

4 Haga clic en el icono de puntos suspensivos para el TPM virtual.

5 Haga clic en **Quitar dispositivo**.

6 Haga clic en **Eliminar** para confirmar que desea quitar el vTPM.

El dispositivo vTPM se marcará para su eliminación.

7 Haga clic en **Aceptar**.

Identificar las máquinas virtuales habilitadas para el módulo de la plataforma de confianza virtual

Puede identificar las máquinas virtuales habilitadas para el uso de un módulo de plataforma de confianza virtual (Virtual Trusted Platform Module, vTPM).

Puede generar una lista de todas las máquinas virtuales del inventario que incluya el nombre de la máquina virtual, el sistema operativo y el estado de vTPM. También puede exportar esta lista a un archivo CSV para su uso en auditorías de cumplimiento.

Procedimiento

1 Conéctese a vCenter Server mediante vSphere Client.

2 Seleccione una instancia de vCenter Server, un host o un clúster.

3 Haga clic en la pestaña **Máquinas virtuales** y seleccione **Máquinas virtuales**.

4 Para ver todas las máquinas virtuales en las que está habilitado un TPM, haga clic en **Administrar columnas** y seleccione **TPM**.

La columna TPM muestra "Presente" en las máquinas virtuales en las que esté habilitado un TPM. Las máquinas virtuales sin TPM se muestran como "No presentes".

5 Para exportar el contenido de una vista de lista de inventario a un archivo CSV, haga clic en **Exportar**.

Ver certificados de dispositivo del módulo de plataforma de confianza virtual

Los dispositivos del módulo de plataforma de confianza virtual (Virtual Trusted Platform Module, vTPM) están preconfigurados con certificados predeterminados, que pueden revisarse.

Requisitos previos

Debe haber una máquina virtual que admita vTPM en su entorno.

Procedimiento

1 Conéctese a vCenter Server mediante vSphere Client.

2 Seleccione un objeto del inventario que sea un objeto primario válido de una máquina virtual, por ejemplo, un host o clúster ESXi.

3 Para identificar las máquinas virtuales con vTPM habilitado, haga clic en **Máquinas virtuales** y, a continuación, haga clic en **Máquinas virtuales**.

   Si es necesario, haga clic en **Administrar columnas** y seleccione **TPM** para mostrar las máquinas virtuales con un TPM "Presente".

4 Seleccione la máquina virtual con el módulo vTPM habilitado cuya información de certificado desee ver.

5 Haga clic en la pestaña **Configurar** de la máquina virtual.

6 En **TPM**, seleccione **Certificados**.

7 Seleccione el certificado y vea su información.

8 (Opcional) Para exportar la información del certificado, haga clic en **Exportar**.

   El certificado se guarda en el disco.

Pasos siguientes

Puede reemplazar el certificado predeterminado por un certificado emitido por una entidad de certificación de terceros (Certificate Authority, CA). Consulte Exportar y reemplazar certificados de dispositivo del Módulo de plataforma de confianza.

Exportar y reemplazar certificados de dispositivo del Módulo de plataforma de confianza

Puede reemplazar el certificado predeterminado incluido en el dispositivo del módulo de plataforma de confianza virtual (vTPM).

Requisitos previos

Debe haber una máquina virtual que admita vTPM en su entorno.

Procedimiento

1 Conéctese a vCenter Server mediante vSphere Client.

2 Seleccione un objeto del inventario que sea un objeto primario válido de una máquina virtual, por ejemplo, un host o clúster ESXi.

3 Seleccione la máquina virtual que admita vTPM en el inventario cuya información de certificado desee reemplazar.

4 Haga clic en la pestaña **Configurar**.

5 En **TPM**, seleccione **Solicitudes de firma**.

6 Seleccione un certificado.

7 Para exportar la información del certificado, haga clic en **Exportar**.

   El certificado se guarda en el disco.

8 Obtenga un certificado emitido por una entidad de certificación (Certificate Authority, CA) de terceros mediante la solicitud de firma del certificado (Certificate Signing Request, CSR) que exportó.

   Puede utilizar cualquier CA de prueba que tenga en el entorno de TI.

9 Cuando tenga el certificado nuevo, reemplace el certificado existente.

   a Haga clic con el botón derecho en la máquina virtual en el inventario cuyo certificado desee modificar y seleccione **Editar configuración**.

   b En el cuadro de diálogo **Editar configuración**, expanda **Dispositivos de seguridad** y, a continuación, expanda **TPM virtual**.

      Aparecen los certificados.

   c Haga clic en **Reemplazar** para el certificado que desea reemplazar.

      Aparece el cuadro de diálogo **Cargar archivo**.

   d En la máquina local, busque el nuevo certificado y cárguelo.

      El nuevo certificado sustituye al certificado predeterminado que incluía el dispositivo vTPM.

   e La información del certificado se actualiza en la lista Certificados.

Proteger sistemas operativos invitados Windows con seguridad basada en la virtualización

12

En vSphere 6.7 y versiones posteriores, puede habilitar la seguridad basada en la virtualización (Virtualization-Based Security, VBS) de Microsoft en los sistemas operativos invitados Windows compatibles.

Microsoft VBS, una función que se introdujo en los sistemas operativos Windows 10 y Windows Server 2016, utiliza la virtualización de hardware y software para mejorar la seguridad del sistema mediante la creación de un subsistema aislado, especializado y restringido por el hipervisor.

VBS permite utilizar las siguientes funciones de seguridad de Windows a fin de proteger el sistema y aislar los datos confidenciales clave del sistema y del usuario para que no se vean comprometidos:

- Protección de credenciales: tiene como objetivo aislar y proteger datos confidenciales clave del sistema y del usuario frente a riesgos.
- Protección de dispositivos: proporciona un conjunto de funciones diseñadas para trabajar juntas con el fin de prevenir y eliminar el malware que se ejecuta en un sistema Windows.
- Integridad de código configurable: garantiza que solo se ejecute código de confianza desde el cargador de arranque en adelante.

Consulte el tema sobre la seguridad basada en la virtualización en la documentación de Microsoft para obtener más información.

Después de habilitar VBS para una máquina virtual a través de vCenter Server, debe habilitar VBS en el sistema operativo invitado Windows.

Lea los siguientes temas a continuación:

Prácticas recomendadas de seguridad basada en la virtualización de vSphere

Siga las prácticas recomendadas de VBS para maximizar la seguridad y la facilidad de administración del entorno de sistema operativo invitado Windows.

Evite problemas siguiendo estas prácticas recomendadas.

Requisitos de hardware de VBS

Utilice el siguiente hardware para VBS:

- Intel
  - CPU Haswell o una versión posterior. Para obtener el mejor rendimiento, utilice la CPU Skylake-EP o una versión posterior.
  - La CPU Ivy Bridge es aceptable.
  - La CPU Sandy Bridge puede provocar un rendimiento lento.
- AMD
  - CPU de la serie Zen 2 (Rome) o posterior.
  - Las CPU más antiguas pueden provocar un rendimiento reducido.

Las mitigaciones para la excepción de comprobación de máquina sobre la vulnerabilidad de cambio de tamaño de página de la CPU de Intel pueden afectar negativamente al rendimiento del sistema operativo invitado cuando VBS está en uso. Para obtener más información, consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/kb/76050.

Compatibilidad de VBS y el sistema operativo invitado Windows

Sobre Intel, VBS es compatible con máquinas virtuales con Windows 10 y Windows Server 2016 y versiones posteriores, aunque las versiones 1607 y 1703 de Windows Server 2016 requieren revisiones. Consulte la documentación de Microsoft sobre compatibilidad de hardware del host de ESXi. El uso de las CPU Intel para VBS requiere vSphere 6.7 o posterior y la versión 14 o posterior del hardware.

En AMD, se admite VBS en máquinas virtuales Windows 10 versión 1809 y Windows 2019 y versiones posteriores. El uso de las CPU AMD para VBS requiere vSphere 7.0 Update 2 o posterior y la versión 19 o posterior del hardware.

Inicialmente, Windows 10 requería habilitar Hyper-V para VBS. Para Windows 10 no es necesario habilitar Hyper-V. Lo mismo se aplica a Windows Server 2016 y versiones posteriores. Para obtener más información, consulte la documentación actual de Microsoft y las *Notas de la versión de VMware vSphere*.

Funciones de VMware no admitidas en VBS

Las siguientes funciones no se admiten en una máquina virtual cuando se habilita VBS:

- Tolerancia a errores
- Acceso directo a PCI
- La adición en caliente de CPU o memoria

Las advertencias de instalación y actualización con VBS

Antes de configurar VBS, debe comprender las siguientes advertencias de instalación y actualización:

- Las máquinas virtuales nuevas configuradas para Windows 10 y Windows Server 2016 y versiones posteriores en versiones de hardware virtual inferiores a 14 se crean mediante BIOS heredado de forma predeterminada. Debe volver a instalar el sistema operativo invitado después de cambiar el tipo de firmware de la máquina virtual desde el BIOS heredado a UEFI.
- Si va a migrar las máquinas virtuales de versiones anteriores de vSphere a vSphere 6.7 o una versión posterior y tiene pensado habilitar VBS en las máquinas virtuales, use UEFI para evitar tener que volver a instalar el sistema operativo.

Activar la seguridad basada en virtualización en una máquina virtual

Puede activar la seguridad basada en la virtualización (VBS) de Microsoft para sistemas operativos invitados Windows compatibles mientras crea una máquina virtual.

La configuración de VBS es un proceso en el que primero se debe activar VBS en la máquina virtual y, posteriormente, en el sistema operativo Windows invitado.

Requisitos previos

Consulte Prácticas recomendadas de seguridad basada en la virtualización de vSphere para conocer las CPU aceptables.

El uso de las CPU Intel para VBS requiere vSphere 6.7 o una versión posterior. Cree una máquina virtual que utilice la versión de hardware 14 o posterior y uno de los siguientes sistemas operativos invitados compatibles:

- Windows 10 (64 bits) o versiones posteriores
- Windows Server 2016 (64 bits) o versiones posteriores

El uso de las CPU AMD para VBS requiere vSphere 7.0 Update 2 o una versión posterior. Cree una máquina virtual que utilice la versión de hardware 19 o posterior y uno de los siguientes sistemas operativos invitados compatibles:

- Windows 10 (64 bits), versión 1809 o versiones posteriores
- Windows Server 2019 (64 bits) o versiones posteriores

Antes de activar VBS, asegúrese de instalar las revisiones más recientes para Windows 10, versión 1809, y Windows Server 2019.

Para obtener más información sobre cómo activar VBS en máquinas virtuales en plataformas AMD, consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/89880.

Procedimiento

1 Conéctese a vCenter Server mediante vSphere Client.

2 Seleccione un objeto del inventario que sea un objeto primario válido de una máquina virtual, por ejemplo, un host o clúster ESXi.

3 Haga clic con el botón derecho en el objeto, seleccione **Nueva máquina virtual** y siga las indicaciones para crear una máquina virtual.

Opción	Acción
Seleccionar un tipo de creación	Cree una máquina virtual.
Seleccionar un nombre y una carpeta	Especifique un nombre y una ubicación de destino.
Seleccionar un recurso informático	Especifique el objeto sobre el que tiene privilegios para crear máquinas virtuales.
Seleccionar almacenamiento	En la directiva de almacenamiento de máquina virtual, seleccione la directiva de almacenamiento. Seleccione un almacén de datos compatible.
Seleccionar compatibilidad	CPU Intel: asegúrese de seleccionar **ESXi 6.7 y versiones posteriores**. CPU AMD: asegúrese de seleccionar **ESXi 7.0 U2 y versiones posteriores**.
Seleccionar un sistema operativo invitado	Seleccione la opción del sistema operativo invitado Windows que mejor se corresponda con la versión del sistema operativo. Activar la casilla **Habilitar seguridad basada en virtualización de Windows**.
Personalizar hardware	Personalice el hardware, por ejemplo, cambiando el tamaño de disco o CPU.
Listo para finalizar	Revise la información y haga clic en **Finalizar**.

Resultados

El mosaico Detalles de la máquina virtual en la pestaña **Resumen** muestra "Seguridad basada en virtualización - Habilitar".

Pasos siguientes

Consulte Activar la seguridad basada en virtualización en el sistema operativo invitado.

Activar la seguridad basada en virtualización en una máquina virtual existente

Puede activar la seguridad basada en la virtualización (VBS) de Microsoft en las máquinas virtuales existentes para sistemas operativos invitados Windows admitidos.

La configuración de VBS es un proceso en el que primero se debe activar VBS en la máquina virtual y, posteriormente, en el sistema operativo invitado.

Nota Las máquinas virtuales nuevas configuradas para Windows 10, Windows Server 2016 y Windows Server 2019 en versiones de hardware inferiores a la versión 14 se deben crear mediante BIOS heredado de forma predeterminada. Si cambia el tipo de firmware de la máquina virtual de BIOS heredado a UEFI, debe volver a instalar el sistema operativo invitado.

Requisitos previos

Consulte Prácticas recomendadas de seguridad basada en la virtualización de vSphere para conocer las CPU aceptables.

El uso de las CPU Intel para VBS requiere vSphere 6.7 o una versión posterior. La máquina virtual debe ser una creada con hardware de versión 14 o posterior y uno de los siguientes sistemas operativos invitados compatibles:

- Windows 10 (64 bits) o versiones posteriores
- Windows Server 2016 (64 bits) o versiones posteriores

El uso de las CPU AMD para VBS requiere vSphere 7.0 Update 2 o una versión posterior. La máquina virtual debe ser una creada con hardware de versión 19 o posterior y uno de los siguientes sistemas operativos invitados compatibles:

- Windows 10 (64 bits), versión 1809 o versiones posteriores
- Windows Server 2019 (64 bits) o versiones posteriores

Antes de activar VBS, asegúrese de instalar las revisiones más recientes para Windows 10, versión 1809, y Windows Server 2019.

Para obtener más información sobre cómo activar VBS en máquinas virtuales en plataformas AMD, consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/89880.

Procedimiento

1 En vSphere Client, desplácese hasta la máquina virtual.

2 Haga clic con el botón derecho en la máquina virtual y seleccione **Editar configuración**.

3 Haga clic en la pestaña **Opciones de máquina virtual**.

4 Active la casilla **Habilitar** para Seguridad basada en virtualización.

5 Haga clic en **Aceptar**.

Resultados

El mosaico Detalles de la máquina virtual en la pestaña **Resumen** muestra "Seguridad basada en virtualización - Habilitar".

Pasos siguientes

Consulte Activar la seguridad basada en virtualización en el sistema operativo invitado.

Activar la seguridad basada en virtualización en el sistema operativo invitado

Puede activar la seguridad basada en la virtualización (VBS) de Microsoft para sistemas operativos invitados Windows admitidos.

Active VBS desde el sistema operativo invitado Windows. Windows configura y aplica VBS a través de un objeto de directiva de grupo (Group Policy Object, GPO). El objeto GPO ofrece la posibilidad de desactivar y activar los diversos servicios, como el arranque seguro, la protección de dispositivos y la protección de credenciales, que ofrece VBS. Ciertas versiones de Windows también requieren que se realice un paso adicional para habilitar la plataforma de Hyper-V.

Consulte la documentación de Microsoft sobre la implementación de la protección de dispositivos para activar la seguridad basada en virtualización si desea obtener más detalles.

Requisitos previos

- Asegúrese de que se haya activado la seguridad basada en virtualización en la máquina virtual.

Procedimiento

1. En Microsoft Windows, edite la directiva de grupo para activar VBS y elegir otras opciones de seguridad relacionadas con VBS.
2. (opcional) Para las versiones de Microsoft Windows inferiores a Redstone 4, en el panel de control Características de Windows, habilite la plataforma de Hyper-V.
3. Reinicie el sistema operativo invitado.

Desactivar la seguridad basada en virtualización

Si ya no utiliza la seguridad basada en virtualización (Virtualization-based Security, VBS) con una máquina virtual, puede desactivarla. Cuando se desactiva VBS en la máquina virtual, las opciones de VBS de Windows permanecen sin modificaciones, pero pueden provocar problemas de rendimiento. Antes de desactivar VBS en la máquina virtual, desactive las opciones de VBS dentro de Windows.

Requisitos previos

Compruebe que la máquina virtual esté apagada.

Procedimiento

1 En vSphere Client, desplácese hasta la máquina virtual que utilice VBS.

   Consulte Identificar máquinas virtuales habilitadas para VBS para obtener ayuda sobre cómo encontrar máquinas virtuales que usen VBS.

2 Haga clic con el botón derecho en la máquina virtual y seleccione **Editar configuración**.

3 Haga clic en **Opciones de máquina virtual**.

4 Anule la selección de la casilla **Habilitar** para Seguridad basada en virtualización.

   Un mensaje le recordará que debe desactivar VBS en el sistema operativo invitado.

5 Haga clic en **Aceptar**.

6 Compruebe que la pestaña **Resumen** de la máquina virtual ya no muestre "Virtualización basada en seguridad - Habilitar" en la descripción del SO invitado.

Identificar máquinas virtuales habilitadas para VBS

Puede identificar las máquinas virtuales que tienen la VBS habilitada para fines de cumplimiento y generación de informes.

Procedimiento

1 Conéctese a vCenter Server mediante vSphere Client.

2 Seleccione un host, un centro de datos o una instancia de vCenter Server en el inventario.

3 Haga clic en la pestaña **Máquinas virtuales** y seleccione **Máquinas virtuales**.

4 Para mostrar la columna **VBS**, haga clic en **Administrar columnas** y seleccione la casilla de verificación **VBS**.

5 Busque "Presente" en la columna **VBS**.

Proteger las redes de vSphere

13

La protección de las redes de vSphere es una parte fundamental de la seguridad del entorno. Los diferentes componentes de vSphere se protegen de varias maneras. Consulte la documentación de *Redes de vSphere* para obtener información detallada sobre las redes del entorno de vSphere.

La seguridad de red para el entorno de vSphere contiene muchas características similares a la protección de un entorno de red física, pero también incluye algunas otras que se aplican solamente a las máquinas virtuales.

Usar firewalls

Agregue protección de firewall a la red virtual mediante la instalación y la configuración de firewalls basados en host en algunas o todas las máquinas virtuales.

Para mejorar la eficiencia, puede configurar redes virtuales o redes Ethernet de máquinas virtuales privadas. En las redes virtuales, se instala un firewall basado en host en una máquina virtual en el encabezado de la red virtual. Este firewall funciona como búfer de protección entre el adaptador de red físico y las máquinas virtuales restantes de la red virtual.

Los firewalls basados en host pueden reducir el rendimiento. Equilibre las necesidades de seguridad con respecto a los objetivos de rendimiento antes de instalar firewalls basados en hosts en las máquinas virtuales en otro lugar de la red virtual.

Consulte Proteger la red con firewalls.

Usar segmentación de red

Mantenga las zonas de máquinas virtuales diferentes dentro de un host en distintos segmentos de red. Al aislar cada zona de máquinas virtuales en su propio segmento de red, es posible minimizar el riesgo de pérdidas de datos entre una zona y la siguiente. Con la segmentación se evitan diversas amenazas, incluida la suplantación del protocolo Address Resolution Protocol (ARP). Con la suplantación de ARP, un atacante manipula la tabla de ARP para reasignar las direcciones MAC e IP, y así obtener acceso al tráfico de red que va al host y procede de él. Los atacantes usan la suplantación de protocolo ARP para generar ataques de tipo "Man in the middle" (MITM), realizar ataques por denegación de servicio (DoS), secuestrar el sistema de destino y desestabilizar la red virtual de otras maneras.

Si la segmentación se planifica minuciosamente, se reducen las posibilidades de que se realicen transmisiones de paquetes entre las zonas de máquinas virtuales. Con la segmentación, por tanto, se evitan los ataques por analizadores de protocolos (sniffer), que se basan en el envío de tráfico de red a la víctima. Asimismo, un atacante no puede usar un servicio que no sea seguro en una zona de máquinas virtuales para acceder a otras zonas del host. El usuario puede elegir entre dos enfoques para implementar la segmentación.

- Use adaptadores de red físicos separados para las zonas de máquinas virtuales a fin de garantizar que las zonas queden aisladas. Probablemente, este método sea el más seguro después de la creación inicial del segmento. Este enfoque es también menos proclive a producir errores de configuración.
- Configure redes de área local virtuales (VLAN) para ayudar a proteger la red. Las VLAN proporcionan casi todas las ventajas de seguridad inherentes en la implementación de redes separadas físicamente sin generar una sobrecarga de hardware. Pueden ahorrarle el coste de tener que implementar y mantener otros dispositivos, el cableado, etc. Consulte Proteger las máquinas virtuales con VLAN.

Evitar el acceso no autorizado a las máquinas virtuales

Los requisitos para proteger las máquinas virtuales suelen ser los mismos que los requisitos para proteger las máquinas físicas.

- Si una red de máquinas virtuales está conectada a una red física, puede quedar expuesta a infracciones, al igual que una red compuesta de máquinas físicas.
- Incluso si no conecta una máquina virtual a la red física, la máquina virtual puede recibir ataques de otras máquinas virtuales.

Las máquinas virtuales permanecen aisladas unas de otras. Una máquina virtual no puede leer ni escribir la memoria de otra máquina virtual, acceder a sus datos, utilizar sus aplicaciones, etc. Sin embargo, dentro de la red, cualquier máquina virtual o un grupo de máquinas virtuales puede seguir siendo el destino del acceso no autorizado de otras máquinas virtuales. Proteja las máquinas virtuales de este tipo de acceso no autorizado.

Para obtener más información sobre cómo proteger las máquinas virtuales, consulte el documento de NIST llamado "Configuración de red virtual segura para la protección de máquinas virtuales (Virtual Machine, VM)" en:

https://csrc.nist.gov/publications/detail/sp/800-125b/final

Lea los siguientes temas a continuación:

- Proteger conmutadores distribuidos y grupos de puertos distribuidos de vSphere
- Proteger las máquinas virtuales con VLAN
- Crear varias redes en un único host ESXi
- Usar el protocolo Internet Protocol Security en hosts ESXi
- Garantizar una configuración de SNMP adecuada en los hosts ESXi
- Prácticas recomendadas de seguridad de redes de vSphere

Proteger la red con firewalls

Los administradores de seguridad usan firewalls para proteger la red o los componentes seleccionados en la red de las intromisiones.

Los firewalls controlan el acceso a los dispositivos dentro de su perímetro mediante el cierre de todos los puertos, excepto los puertos que el administrador designa explícita o implícitamente como autorizados. Los puertos que el administrador abre permiten el tráfico entre dispositivos en diferentes lados del firewall.

Importante El firewall de ESXi en ESXi 5.5 y versiones posteriores no permite filtrar el tráfico de vMotion por red. Por lo tanto, se deben instalar reglas en el firewall externo para que no se puedan establecer conexiones entrantes con el socket de vMotion.

En un entorno de máquina virtual, se puede planear la distribución de los firewalls entre los componentes.

- Firewalls entre máquinas físicas, tales como los sistemas vCenter Server y los hosts ESXi.
- Los firewalls entre una máquina virtual y otra, por ejemplo, entre una máquina virtual que actúa como servidor web externo y una máquina virtual conectada a la red interna de la empresa.
- Firewalls entre una máquina física y una máquina virtual, como cuando se coloca un firewall entre una tarjeta de adaptador de red física y una máquina virtual.

El modo de usar firewalls en la configuración de ESXi depende de cómo se planea utilizar la red y qué tan seguro debe ser un componente determinado. Por ejemplo, si crea una red virtual en la que cada máquina virtual está dedicada a ejecutar un conjunto de pruebas de referencia diferente para el mismo departamento, el riesgo de que se produzca un acceso no deseado de una máquina virtual a la siguiente es mínimo. Por lo tanto, no se necesita una configuración en la que haya firewalls entre las máquinas virtuales. Sin embargo, para evitar la interrupción de la ejecución de una prueba por parte de un host externo, puede configurar un firewall en el punto de entrada de la red virtual a fin de proteger todo el conjunto de máquinas virtuales.

Para obtener la lista de todos los puertos y protocolos compatibles en los productos de VMware, incluidos vSphere y vSAN, consulte la herramienta VMware Ports and Protocols™ en https://ports.vmware.com/. Puede buscar puertos por producto de VMware, crear una lista de puertos personalizada e imprimir o guardar listas de puertos.

Firewalls para configuraciones con vCenter Server

Si se accede a los hosts ESXi a través de vCenter Server, generalmente se protege vCenter Server con un firewall.

Los firewalls deben estar en el punto de entrada. El firewall puede estar entre los clientes y vCenter Server, o bien tanto vCenter Server como los clientes pueden estar detrás de un firewall.

Para obtener la lista de todos los puertos y protocolos compatibles en los productos de VMware, incluidos vSphere y vSAN, consulte la herramienta VMware Ports and Protocols™ en https://ports.vmware.com/. Puede buscar puertos por producto de VMware, crear una lista de puertos personalizada e imprimir o guardar listas de puertos.

Las redes configuradas con vCenter Server pueden recibir comunicaciones a través de vSphere Client, otros clientes de UI o clientes que utilizan vSphere API. Durante un funcionamiento normal, vCenter Server escucha los datos de sus hosts y clientes administrados en los puertos designados. vCenter Server también asume que sus hosts administrados escuchan datos de vCenter Server en los puertos designados. Si hay un firewall entre cualquiera de estos elementos, el firewall debe tener puertos abiertos para admitir la transferencia de datos.

También se pueden incluir firewalls en otros puntos de acceso de la red, según el uso de la red y el nivel de seguridad que requieren los clientes. Seleccione las ubicaciones de los firewalls según los riesgos de seguridad de la configuración de red. Las siguientes ubicaciones de firewall se utilizan comúnmente.

- Entre vSphere Client o un cliente de administración de redes externo y vCenter Server.
- Si sus usuarios acceden a las máquinas virtuales a través de un explorador web, entre el explorador web y el host ESXi.
- Si sus usuarios acceden a las máquinas virtuales a través de vSphere Client, entre vSphere Client y el host ESXi. Esta conexión es adicional a la conexión entre vSphere Client y vCenter Server, y requiere un puerto diferente.
- Entre vCenter Server y los hosts ESXi.
- Entre los hosts ESXi de la red. A pesar de que el tráfico entre hosts generalmente se considera confiable, puede agregar firewalls entre ellos si sospecha que hay infracciones de seguridad entre una máquina y la otra.

  Si agrega firewalls entre hosts ESXi y tiene pensado migrar las máquinas virtuales entre ellos, abra los puertos en cualquier firewall que divida el host de origen de los host de destino.
- Entre los hosts ESXi y el almacenamiento de red, como el almacenamiento NFS o de iSCSI. Estos puertos no son exclusivos de VMware. Configúrelos de acuerdo con las especificaciones de la red.

Conexión con vCenter Server mediante un firewall

Abra el puerto TCP 443 en el firewall para que vCenter Server pueda recibir datos.

De forma predeterminada, vCenter Server usa el puerto TCP 443 para escuchar la transferencia de datos de sus clientes. Si se usa un firewall entre vCenter Server y sus clientes, es necesario configurar una conexión a través de la cual vCenter Server pueda recibir los datos de sus clientes. La configuración del firewall depende de lo que se use en el sitio. Solicite información al administrador del sistema de firewall local.

Conectar hosts ESXi mediante firewalls

Si tiene un firewall entre los hosts ESXi y vCenter Server, asegúrese de que los hosts administrados puedan recibir datos.

Para configurar una conexión a fin de recibir datos, abra los puertos para el tráfico proveniente de los servicios, como vSphere High Availability, vMotion y vSphere Fault Tolerance. Consulte Configurar el firewall de ESXi para ver una explicación de los archivos de configuración, del acceso de vSphere Client y de los comandos de firewall. Para obtener una lista de puertos, consulte la herramienta VMware Ports and Protocols ™ en https://ports.vmware.com.

Firewalls para configuraciones sin vCenter Server

Si el entorno no incluye vCenter Server, los clientes pueden conectarse directamente a la red ESXi.

Un host independiente ESXi se pueden conectar de varias formas.

- VMware Host Client
- Interfaz de ESXCLI
- vSphere Web Services SDK o vSphere Automation SDK
- Clientes de terceros

Los requisitos de firewall para los hosts independientes son similares a los requisitos aplicables cuando hay una instancia de vCenter Server.

- Utilice un firewall para proteger la capa ESXi o, según la configuración, los clientes y la capa ESXi. El firewall ofrece una protección básica para la red.
- La concesión de licencias en este tipo de configuración es parte del paquete de ESXi que instala en cada uno de los hosts. Debido a que la licencia reside en ESXi, no es necesario contar con un servidor de licencia distinto con un firewall.

Se pueden configurar puertos de firewall mediante ESXCLI o VMware Host Client. Consulte *Administrar un host único de vSphere: VMware Host Client*.

Conectar con la consola de la máquina virtual mediante un firewall

Algunos puertos deben estar abiertos para que el usuario y el administrador se comuniquen con la consola de la máquina virtual. Los puertos que deben estar abiertos dependen del tipo de consola de máquina virtual y de si se establece la conexión mediante vCenter Server con vSphere Client o directamente con el host ESXi desde VMware Host Client.

Para obtener más información sobre los puertos, su propósito y su clasificación (entrantes, salientes o bidireccionales), consulte la herramienta VMware Ports and Protocols™ en https://ports.vmware.com.

Conectarse a una consola de máquina virtual basada en explorador mediante vSphere Client

Cuando se conecta con vSphere Client, se conecta siempre al sistema vCenter Server que administra el host ESXi, y se accede desde allí a la consola de máquina virtual.

Si utiliza vSphere Client y se conecta a una consola de máquina virtual basada en explorador, el acceso siguiente debe ser posible:

- El firewall debe permitir que vSphere Client acceda a vCenter Server en el puerto 443.
- El firewall debe permitir que vCenter Server acceda al host ESXi en el puerto 902.

Conectarse a VMware Remote Console mediante vSphere Client

Si utiliza vSphere Client y se conecta a VMware Remote Console (VMRC), el acceso siguiente debe ser posible:

- El firewall debe permitir que vSphere Client acceda a vCenter Server en el puerto 443.
- El firewall debe permitir que VMRC acceda a vCenter Server en el puerto 443 y al host ESXi en el puerto 902 en las versiones de VMRC anteriores a 11.0, y en el puerto 443 en la versión 11.0 y posteriores de VMRC. Para obtener más información sobre la versión 11.0 de VMRC y los requisitos de puerto de ESXi, consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/76672.

Conexión directa a hosts ESXi con VMware Host Client

Es posible utilizar la consola de máquina virtual de VMware Host Client si se conecta directamente a un host ESXi.

Nota No utilice VMware Host Client para conectarse directamente a hosts administrados por un sistema vCenter Server. Si hace cambios en esos hosts desde VMware Host Client, se producirá inestabilidad en el entorno.

El firewall debe permitir el acceso al host ESXi en los puertos 443 y 902.

VMware Host Client utiliza el puerto 902 para ofrecer una conexión para las actividades de MKS del sistema operativo invitado en las máquinas virtuales. A través de este puerto, los usuarios interactúan con los sistemas operativos invitados y las aplicaciones de la máquina virtual. VMware no admite la configuración de otro puerto para esta función.

Proteger el conmutador físico en hosts ESXi

Proteja el conmutador físico de cada host ESXi para evitar que los atacantes tengan acceso al host y sus máquinas virtuales.

Para optimizar la protección de los hosts, compruebe que los puertos de conmutadores físicos estén configurados con el árbol de expansión desactivado, y que la opción de no negociación esté configurada para los vínculos troncales entre conmutadores físicos externos y conmutadores virtuales en el modo de etiquetado de conmutador virtual (VST).

Procedimiento

1 Inicie sesión en el conmutador físico y compruebe que el protocolo de árbol de expansión esté desactivado o que el puerto rápido esté configurado para todos los puertos de conmutadores físicos conectados a los hosts ESXi.

2 Para las máquinas virtuales que hacen puente y enrutamiento, compruebe periódicamente que el primer puerto de conmutador físico ascendente esté configurado con las opciones de protección de BPDU y puerto rápido desactivadas, y con el protocolo de árbol de expansión activado.

   Para evitar posibles ataques de denegación de servicio (DoS) en el conmutador físico, puede activar el filtro de BPDU invitado en los hosts ESXi.

3 Inicie sesión en el conmutador físico y asegúrese de que el protocolo Dynamic Trunking Protocol (DTP) no esté activado en los puertos de conmutadores físicos conectados a los hosts ESXi.

4 De forma regular, revise los puertos de conmutadores físicos para asegurarse de que estén correctamente configurados como puertos troncales si están conectados a los puertos de enlace troncal de VLAN de conmutadores virtuales.

Protección de puertos de conmutadores estándar con directivas de seguridad

El grupo de puertos de VMkernel o el grupo de puertos de máquinas virtuales de un conmutador estándar tienen una directiva de seguridad configurable. La directiva de seguridad determina el nivel de seguridad con que se aplica la protección contra ataques de suplantación o intercepción en máquinas virtuales.

Al igual que ocurre con los adaptadores de red física, los adaptadores de red de máquina virtual pueden suplantar otra máquina virtual. La suplantación es un riesgo de seguridad.

- Una máquina virtual puede enviar tramas que parezcan ser de otra máquina de modo que reciba tramas de la red que estén destinadas a esa máquina.
- Un adaptador de red de máquina virtual puede configurarse para que reciba tramas destinadas a otras máquinas.

Al agregar un grupo de puertos VMkernel o un grupo de puertos de máquinas virtuales a un conmutador estándar, ESXi configura una directiva de seguridad para los puertos del grupo. Esta directiva de seguridad se puede utilizar para garantizar que el host evite que los sistemas operativos invitados de sus máquinas virtuales suplanten a otras máquinas en la red. El sistema operativo invitado que lleve a cabo la suplantación no detectará que se evitó la suplantación.

La directiva de seguridad determina el nivel de seguridad con que se aplica la protección contra ataques de suplantación o intercepción en máquinas virtuales. Para utilizar correctamente la configuración en el perfil de seguridad, consulte la sección de la directiva de seguridad en la publicación *Redes de vSphere*. En esta sección se explica:

- El modo en el que los adaptadores de red de máquina virtual controlan las transmisiones.
- El modo en el que se manipulan los ataques en este nivel.

Proteger conmutadores estándar de vSphere

Puede proteger el tráfico del conmutador estándar contra ataques de Capa 2 restringiendo algunos de los modos de dirección MAC de los adaptadores de red de máquina virtual.

Cada adaptador de red de máquina virtual tiene una dirección MAC inicial y una dirección MAC efectiva.

Dirección MAC inicial

La dirección MAC inicial se asigna con la creación del adaptador. Si bien la dirección MAC inicial puede volver a configurarse desde afuera del sistema operativo invitado, este sistema no puede modificarla.

Dirección MAC efectiva

Cada adaptador tiene una dirección MAC efectiva que filtra el tráfico de red entrante con una dirección MAC de destino distinta de la dirección MAC efectiva. El sistema operativo invitado es responsable de configurar la dirección MAC efectiva y, por lo general, hace coincidir la dirección MAC efectiva con la dirección MAC inicial.

Qué sucede al crear un adaptador de red de máquina virtual

Al crear un adaptador de red de máquina virtual, la dirección MAC efectiva y la dirección MAC inicial son iguales. El sistema operativo invitado puede modificar la dirección MAC efectiva con otro valor en cualquier momento. Si el sistema operativo modifica la dirección MAC efectiva, su adaptador de red recibe el tráfico de red destinado para la nueva dirección MAC.

Cuando se envían paquetes a través del adaptador de red, el sistema operativo invitado por lo general coloca su propia dirección MAC efectiva de adaptador en el campo de la dirección MAC de origen de las tramas Ethernet. Coloca la dirección MAC del adaptador de red receptor en el campo de la dirección MAC de destino. El adaptador receptor acepta los paquetes únicamente si la dirección MAC de destino del paquete coincide con su propia dirección MAC efectiva.

El sistema operativo puede enviar tramas con una dirección MAC de origen suplantada. Por lo tanto, un sistema operativo puede suplantar a un adaptador de red que haya autorizado la red receptora y llevar a cabo ataques maliciosos en los dispositivos de una red.

Usar directivas de seguridad para proteger puertos y grupos

Puede proteger el tráfico virtual contra ataques de suplantación e intercepción de la Capa 2 si configura una directiva de seguridad en los puertos o grupos de puertos.

La directiva de seguridad en los puertos y grupos de puertos distribuidos incluye las siguientes opciones:

- Cambios en la dirección MAC (consulte Cambios de dirección MAC).
- Modo promiscuo (consulte Operación en modo promiscuo).
- Transmisiones falsificadas (consulte Transmisiones falsificadas).

Puede ver y cambiar la configuración predeterminada si selecciona el conmutador virtual asociado con el host desde vSphere Client. Consulte el documento *Redes de vSphere*.

Cambios de dirección MAC

La directiva de seguridad de un conmutador virtual incluye la opción **Cambios de dirección MAC**. Esta opción permite que las máquinas virtuales reciban tramas con una dirección Mac diferente de la configurada en VMX.

Cuando la opción **Cambios de dirección MAC** está establecida en **Aceptar**, ESXi acepta las solicitudes para cambiar la dirección MAC efectiva de una máquina virtual por una dirección diferente a la inicial.

Cuando la opción **Cambios de dirección MAC** está establecida en **Rechazar**, ESXi no admite las solicitudes para cambiar la dirección MAC efectiva de una máquina virtual por una dirección diferente a la inicial. Esta configuración protege el host de la suplantación de MAC. El puerto que utilizó el adaptador de la máquina virtual para enviar la solicitud se desactiva, y el adaptador de la máquina virtual no recibe más tramas hasta que la dirección MAC efectiva coincida con la dirección MAC inicial. El sistema operativo invitado no detecta el rechazo de la solicitud de cambio de dirección MAC.

Nota El iniciador iSCSI confía en poder obtener los cambios en la dirección MAC a partir de determinados tipos de almacenamiento. Si utiliza iSCSI de ESXi con almacenamiento iSCSI, establezca la opción **Cambios de dirección MAC** en **Aceptar**.

En ciertos casos, puede que realmente necesite que más de un adaptador tenga la misma dirección MAC en una red (por ejemplo, si utiliza el equilibrio de carga de red de Microsoft en modo de unidifusión). Cuando el equilibrio de carga de red de Microsoft se utiliza en el modo de multidifusión estándar, los adaptadores no comparten las direcciones MAC.

Nota A partir de vSphere 7.0, los valores predeterminados para **Transmisiones falsificadas** y **Cambios de dirección MAC** se han cambiado a Rechazar en lugar de Aceptar. Póngase en contacto con el proveedor de almacenamiento para validarlo.

Transmisiones falsificadas

La opción **Transmisiones falsificadas** afecta el tráfico que se transmite desde una máquina virtual.

Cuando la opción **Transmisiones falsificadas** está establecida en **Aceptar**, ESXi no compara las direcciones MAC de origen y efectivas.

Para evitar la suplantación de MAC, puede establecer la opción **Transmisiones falsificadas** en **Rechazar**. Si lo hace, el host compara la dirección MAC de origen que transmite el sistema operativo invitado con la dirección MAC efectiva de su adaptador de máquina virtual para ver si coinciden. Si las direcciones no coinciden, el host ESXi descarta el paquete.

El sistema operativo invitado no detecta que su adaptador de máquina virtual no puede enviar paquetes con la dirección MAC suplantada. El host ESXi intercepta los paquetes con direcciones suplantadas antes de que estos se envíen, y el sistema operativo invitado puede asumir que los paquetes se descartan.

Nota A partir de vSphere 7.0, los valores predeterminados para **Transmisiones falsificadas** y **Cambios de dirección MAC** se han cambiado a Rechazar en lugar de Aceptar.

Operación en modo promiscuo

El modo promiscuo quita el filtrado de recepción que realiza el adaptador de la máquina virtual a fin de que el sistema operativo invitado reciba todo el tráfico que se observa en la conexión. De forma predeterminada, el adaptador de la máquina virtual no puede operar en modo promiscuo.

A pesar de que el modo promiscuo puede ser útil para hacer un seguimiento de la actividad de la red, es un modo de operación no seguro, ya que cualquier adaptador en modo promiscuo tiene acceso a los paquetes, incluso si algunos de estos paquetes se reciben solamente en un adaptador de red en particular. Esto significa que un administrador o un usuario raíz que estén en una máquina virtual pueden ver potencialmente el tráfico destinado a otros sistemas operativos host o invitados.

Consulte el tema sobre cómo configurar la directiva de seguridad para un conmutador estándar de vSphere o un grupo de puertos estándar en la documentación de *Redes de vSphere*, para obtener información sobre cómo configurar el adaptador de máquina virtual para el modo promiscuo.

Nota En ciertas ocasiones, es posible que tenga una razón válida para configurar un conmutador virtual estándar o distribuido para operar en modo promiscuo, por ejemplo, si está ejecutando un software de detección de intrusiones de red o un analizador de protocolos (sniffer).

Protección de conmutador estándar y VLAN

Los conmutadores estándar de VMware ofrecen elementos de protección contra ciertas amenazas para la seguridad de VLAN. Debido a la forma en que se diseñan, los conmutadores

estándar protegen las VLAN contra una variedad de ataques, muchos de los cuales implican saltos de VLAN.

Contar con esta protección no garantiza que la configuración de la máquina virtual sea invulnerable a otros tipos de ataques. Por ejemplo, los conmutadores estándar no protegen la red física frente a estos ataques: protegen solo la red virtual.

Los conmutadores estándar y las VLAN pueden ofrecer protección contra los siguientes tipos de ataques.

Debido a que con el tiempo surgen nuevas amenazas de seguridad, no considere que esta lista de ataques está completa. Revise con regularidad los recursos de seguridad de VMware en la Web para obtener información sobre seguridad, alertas de seguridad recientes y tácticas de seguridad de VMware.

Desbordamiento de MAC

El desbordamiento de MAC desborda un conmutador con paquetes que contienen direcciones MAC etiquetadas como provenientes de diferentes orígenes. Muchos conmutadores utilizan una tabla de memoria de contenido direccionable que permite conocer y almacenar la dirección de origen para cada paquete. Cuando la tabla está completa, el conmutador puede entrar en un estado completamente abierto en el que todos los paquetes entrantes se difunden a todos los puertos; esto permite al atacante ver todo el tráfico del conmutador. Dicho estado puede resultar en la pérdida de paquetes en todas las VLAN.

Aunque los conmutadores estándar de VMware almacenan una tabla de direcciones MAC, no obtienen estas del tráfico observable y no son vulnerables a este tipo de ataque.

Ataques de etiquetado de ISL y 802.1q

Los ataques de etiquetado de ISL y 802.1q fuerzan a un conmutador a redirigir las tramas de una VLAN a otra; para ello, se engaña al conmutador para que actúe como un enlace troncal y difunda el tráfico hacia otras VLAN.

Los conmutadores estándar de VMware no llevan a cabo el enlace troncal dinámico requerido para este tipo de ataque y, por lo tanto, no son vulnerables.

Ataques de doble encapsulación

Los ataques de doble encapsulación se producen cuando un atacante crea un paquete de doble encapsulado donde el identificador de VLAN en la etiqueta interior es diferente del identificador de VLAN en la etiqueta exterior. Para lograr la compatibilidad con versiones anteriores, las VLAN nativas quitan la etiqueta exterior de los paquetes transmitidos a menos que se configure de otro modo. Cuando un conmutador de VLAN nativa quita la etiqueta exterior, queda solo la etiqueta interior, que enruta el paquete a una VLAN diferente de la que está identificada en la etiqueta exterior ahora faltante.

Los conmutadores estándar de VMware sueltan todas las tramas de doble encapsulado que una máquina virtual intenta enviar y lo hacen en un puerto configurado para una VLAN específica. Por lo tanto, no son vulnerables a este tipo de ataque.

Ataques de fuerza bruta de multidifusión

Implican el envío de gran cantidad de tramas de multidifusión a una VLAN conocida casi al mismo tiempo a fin de sobrecargar el conmutador de modo que, por error, permita que algunas de las tramas se difundan a otras VLAN.

Los conmutadores estándar de VMware no permiten que las tramas abandonen el dominio de difusión correcto (VLAN) y no son vulnerables a este tipo de ataque.

Ataques de árbol de expansión

Los ataques de árbol de expansión se dirigen al protocolo Spanning-Tree Protocol (STP), que se utiliza para controlar el puente entre las partes de la red LAN. El atacante envía paquetes de Bridge Protocol Data Unit (BPDU) que intentan cambiar la topología de la red y se establecen a sí mismos como el puente raíz. Como puente raíz, el atacante puede capturar el contenido de las tramas difundidas.

Los conmutadores estándar de VMware no son compatibles con el protocolo STP y no son vulnerables a este tipo de ataque.

Ataques de trama aleatoria

Los ataques de trama aleatoria implican enviar grandes cantidades de paquetes donde las direcciones de origen y destino permanecen iguales, pero se cambia de forma aleatoria la longitud, el tipo o el contenido de los campos. El objetivo de este ataque es forzar a los paquetes a que, por error, se vuelvan a enrutar a una VLAN diferente.

Los conmutadores estándar de VMware no son vulnerables a este tipo de ataque.

Proteger conmutadores distribuidos y grupos de puertos distribuidos de vSphere

Los administradores tienen varias opciones para proteger instancias de vSphere Distributed Switch en el entorno de vSphere.

Las mismas reglas se aplican a las VLAN tanto en una instancia de vSphere Distributed Switch como en un conmutador estándar. Para obtener más información, consulte Protección de conmutador estándar y VLAN.

Procedimiento

1 Para los grupos de puertos distribuidos con enlace estático, desactive la característica de expansión automática.

   La expansión automática está activada de forma predeterminada.

Para desactivar Expansión automática, configure la propiedad `autoExpand` en el grupo de puertos distribuidos con vSphere Web Services SDK o con una interfaz de línea de comandos. Consulte la documentación de *vSphere Web Services SDK*.

2 Asegúrese de que todos los identificadores de VLAN privadas de vSphere Distributed Switch estén documentados detalladamente.

3 Si utiliza el etiquetado de VLAN en un dvPortgroup, los identificador de VLAN deben coincidir con los identificadores de los conmutadores ascendentes externos con reconocimiento de VLAN. Si los identificadores de VLAN no están registrados correctamente, la reutilización incorrecta de identificadores puede permitir tráfico no deseado. De forma similar, la presencia de identificadores de VLAN incorrectos o faltantes puede hacer que el tráfico no pase entre las máquinas físicas y virtuales.

4 Asegúrese de que no haya puertos sin utilizar en un grupo de puertos virtuales asociado con vSphere Distributed Switch.

5 Etiquete todos los conmutadores distribuidos de vSphere.

Los conmutadores distribuidos de vSphere asociados con un host ESXi requieren un cuadro de texto para sus nombres. Esta etiqueta sirve como descriptor funcional del conmutador, al igual que el nombre de host asociado con un conmutador físico. La etiqueta de vSphere Distributed Switch indica la función o la subred IP del conmutador Por ejemplo, puede etiquetar el conmutador como interno para indicar que solo sirve para las redes internas del conmutador virtual privado de una máquina virtual. El tráfico no pasa a través de los adaptadores de red física.

6 Desactive la comprobación de estado de la red en los conmutadores distribuidos de vSphere si no la utiliza de forma activa.

La comprobación de estado de la red está desactivada de forma predeterminada. Una vez activada, los paquetes de comprobación de estado contienen información sobre el host, el conmutador y el puerto que podría utilizar un atacante. Utilice la comprobación de estado de la red solo para tareas de solución de problemas y desactívela al finalizar.

7 Puede proteger el tráfico virtual contra ataques de suplantación e intercepción de la Capa 2 si configura una directiva de seguridad en los puertos o grupos de puertos.

La directiva de seguridad en los puertos y grupos de puertos distribuidos incluye las siguientes opciones:

- Cambios en la dirección MAC (consulte Cambios de dirección MAC).
- Modo promiscuo (consulte Operación en modo promiscuo).
- Transmisiones falsificadas (consulte Transmisiones falsificadas).

Para ver y cambiar la configuración actual, seleccione **Administrar grupos de puertos distribuidos** en el menú contextual y, a continuación, seleccione **Seguridad** en el asistente. Consulte la documentación de *Redes de vSphere*.

Proteger las máquinas virtuales con VLAN

La red puede ser una de las partes más vulnerables de un sistema. La red de máquinas virtuales necesita tanta protección como una red física. La utilización de VLAN puede mejorar la seguridad de las redes del entorno.

Las VLAN se encuentran en un esquema de redes estándar IEEE, con métodos de etiquetado específicos que permiten el enrutamiento de los paquetes únicamente hacia los puertos que forman parte de la VLAN. Cuando se las configura correctamente, las VLAN constituyen un medio confiable para proteger un conjunto de máquinas virtuales contra intrusiones accidentales o maliciosas.

Las VLAN permiten segmentar una red física de modo que dos máquinas de la red no puedan transmitirse paquetes entre ellas a menos que formen parte de la misma VLAN. Por ejemplo, las transacciones y los registros contables son algunos de los datos internos más confidenciales de una empresa. En una empresa cuyos empleados de los departamentos de ventas, envíos y contabilidad utilizan máquinas virtuales en la misma red física, es posible proteger las máquinas virtuales del departamento contable mediante la configuración de las VLAN.

Figura 13-1. Esquema de muestra de una VLAN

En esta configuración, todos los empleados del departamento contable utilizan máquinas virtuales en la VLAN A y los empleados de ventas utilizan máquinas virtuales en la VLAN B.

El enrutador reenvía los paquetes que contienen los datos contables a los conmutadores. Estos paquetes se etiquetan para la distribución en la VLAN A únicamente. Por lo tanto, los datos quedan confinados al dominio de difusión A y no pueden enrutarse al dominio de difusión B a menos que se configure al enrutador para hacerlo.

Esta configuración de VLAN impide que los empleados de ventas intercepten los paquetes destinados al departamento contable. También evita que el departamento contable reciba paquetes destinados al grupo de ventas. Las máquinas virtuales atendidas por un único conmutador virtual pueden encontrarse en diferentes VLAN.

Consideraciones de seguridad para VLAN

La forma de configurar VLAN para proteger partes de una red depende de factores tales como el sistema operativo invitado y el tipo de configuración del equipo de red.

ESXi cuenta con una implementación completa de VLAN compatibles con IEEE 802.1q VLAN. VMware no puede hacer recomendaciones específicas sobre el modo de configurar las VLAN, pero hay algunos factores que deben considerarse al usar la implementación de VLAN como parte de la directiva de cumplimiento de seguridad.

Proteger las VLAN

Los administradores tienen varias opciones para proteger las VLAN en el entorno de vSphere.

Procedimiento

1. Asegúrese de que los grupos de puertos no estén configurados con valores de la VLAN reservados para los conmutadores físicos ascendentes.

   No establezca los identificadores de la VLAN con valores reservados para el conmutador físico.

2. Compruebe que los grupos de puertos no estén configurados en la VLAN 4095 a menos que esté utilizando el etiquetado de invitado virtual (VGT).

   Hay tres tipos de etiquetado de VLAN en vSphere:

   - Etiquetado de conmutador externo (EST)
   - Etiquetado de conmutador virtual (VST): el conmutador virtual etiqueta con el identificador de VLAN configurado el tráfico que entra en las máquinas virtuales asociadas y quita la etiqueta de VLAN del tráfico saliente. Para configurar el modo VST, asigne un identificador de VLAN entre 1 y 4094.
   - Etiquetado de invitado virtual (VGT): las máquinas virtuales controlan el tráfico de VLAN. Para activar el modo VGT, establezca el identificador de VLAN en 4095. En un conmutador distribuido, también puede permitir el tráfico de máquinas virtuales en función de su VLAN mediante la opción **Enlace troncal de VLAN**.

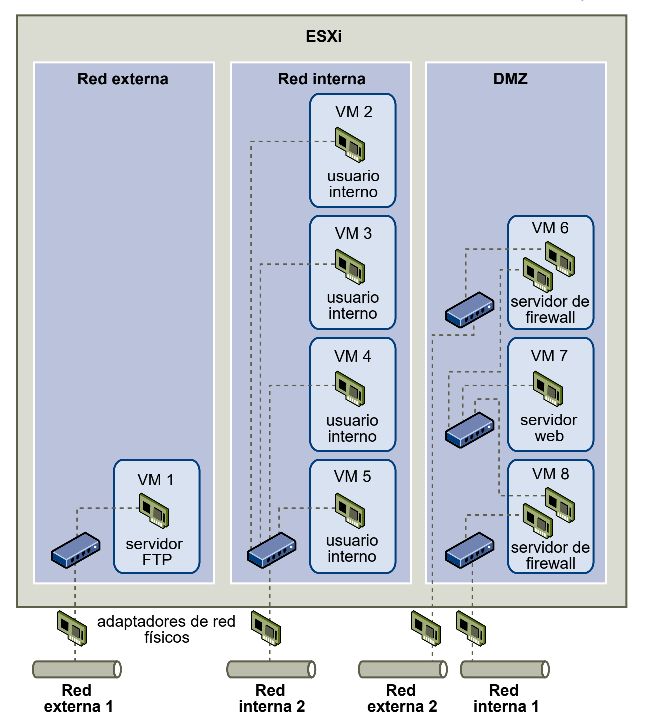
En un conmutador estándar, puede configurar el modo de redes de VLAN en el nivel del conmutador o del grupo de puertos. En un conmutador distribuido, puede hacerlo en el nivel del puerto o del grupo de puertos distribuidos.

3 Asegúrese de que todas las VLAN de cada conmutador virtual estén completamente documentadas y que cada conmutador virtual tenga todas las VLAN requeridas y solamente esas.

Crear varias redes en un único host ESXi

El diseño del sistema ESXi permite conectar algunos grupos de máquinas virtuales a la red interna, otros a la red externa y otros a ambos, todos en el mismo host. Esta capacidad es una extensión del aislamiento básico de máquinas virtuales combinado con la utilización bien planificada de características de redes virtuales.

Figura 13-2. Redes externas, redes internas y una DMZ configuradas en un único host ESXi



En la figura, el administrador de sistema configuró un host en tres zonas de máquinas virtuales diferentes: servidor FTP, máquinas virtuales internas y DMZ. Cada zona tiene una función única.

Zona de servidor FTP

La máquina virtual 1 está configurada con el software FTP y actúa como área de retención de los datos enviados hacia los recursos externos y desde estos, como formularios y documentación localizados por un proveedor.

Esta máquina virtual solo está asociada con una red externa. Tiene su propio conmutador virtual y su propio adaptador de red físico que la conectan a la red externa 1. Esta red está dedicada a los servidores que usa la empresa para recibir datos de orígenes externos. Por ejemplo, la empresa utiliza la red externa 1 para recibir tráfico FTP de los proveedores, y permite a estos últimos acceder a los datos almacenados en servidores disponibles de forma externa a través de FTP. Además de atender a la máquina virtual 1, la red externa 1 se encarga de los servidores FTP configurados en diferentes hosts ESXi en todo el sitio.

Debido a que la máquina virtual 1 no comparte un conmutador virtual o un adaptador de red físico con ninguna máquina virtual del host, las otras máquinas virtuales residentes no pueden transmitir paquetes a la red de la máquina virtual 1 ni recibir paquetes de ella. Esta restricción evita los ataques por analizadores de protocolos (sniffer), que se basan en el envío de tráfico de red a la víctima. Otro factor más importante es que un atacante no puede utilizar la vulnerabilidad natural de FTP para acceder a ninguna de las otras máquinas virtuales del host.

Zona de red interna

Las máquinas virtuales 2 a 5 están reservadas para la utilización interna. Estas máquinas virtuales procesan y almacenan datos privados de la empresa, como registros médicos, declaraciones legales e investigaciones de fraude. Por lo tanto, los administradores del sistema deben garantizar el nivel más alto de protección de estas máquinas virtuales.

Estas máquinas virtuales se conectan a la red interna 2 mediante un conmutador virtual y un adaptador de red propios. La red interna 2 está reservada para la utilización interna por parte del personal, por ejemplo, procesadores de reclamos, abogados internos o tasadores.

Las máquinas virtuales 2 a 5 pueden comunicarse entre sí mediante el conmutador virtual, y con máquinas internas de otros lugares de la red interna 2 mediante el adaptador de red físico. Sin embargo, no pueden comunicarse con máquinas externas. Al igual que con el servidor FTP, estas máquinas virtuales no pueden enviar paquetes a las redes de las otras máquinas virtuales ni recibir paquetes de ellas. De forma similar, las otras máquinas virtuales del host no pueden enviar paquetes a las máquinas virtuales 2 a 5 ni recibir paquetes de ellas.

Zona DMZ

Las máquinas virtuales 6 a 8 se configuran como una DMZ que utiliza el grupo de comercialización para publicar el sitio web externo de la empresa.

Este grupo de máquinas virtuales se asocia con la red externa 2 y la red interna 1. La empresa utiliza la red externa 2 para admitir los servidores web que utilizan los departamentos de comercialización y finanzas para alojar el sitio web de la empresa y otras características web para usuarios externos. La red interna 1 es el medio que utiliza el departamento de comercialización para publicar contenido en el sitio web de la empresa, publicar descargas y mantener servicios como los foros de usuarios.

Debido a que estas redes están separadas de la red externa 1 y la red interna 2, y las máquinas virtuales no tienen puntos de contacto compartidos (conmutadores o adaptadores), no existe riesgo de ataque hacia o desde el servidor FTP o el grupo de máquinas virtuales internas.

Ventajas de usar zonas de máquinas virtuales

Al lograr el aislamiento de máquinas virtuales, configurar correctamente los conmutadores virtuales y mantener la separación de las redes, puede alojar las tres zonas de máquinas virtuales en el mismo host ESXi y estar seguro de que no se producirán vulneraciones de datos o recursos.

La empresa aplica el aislamiento en los grupos de máquinas virtuales mediante la utilización de varias redes internas y externas, y se asegura de que los conmutadores virtuales y los adaptadores de red físicos de cada grupo se encuentren separados de esos grupos o de otros.

Gracias a que ninguno de estos conmutadores virtuales favorece zonas de máquinas virtuales sobre las demás, se logra eliminar el riesgo de pérdida de paquetes de una zona a la otra. Debido a su diseño, un conmutador virtual no puede perder paquetes directamente en otro conmutador virtual. La única forma de que los paquetes pasen de un conmutador virtual a otro es en estas circunstancias:

- Los conmutadores virtuales están conectados a la misma LAN física.
- Los conmutadores virtuales se conectan a una máquina virtual común, que se puede utilizar para transmitir paquetes.

Ninguna de estas condiciones se cumple en la configuración de ejemplo. Si desea comprobar que no existen rutas de acceso a conmutadores virtuales comunes, revise la distribución de conmutadores de red de vSphere Client para buscar posibles puntos de contacto compartidos.

Para proteger los recursos de las máquinas virtuales, configure una reserva de recursos y un límite para cada máquina virtual. De esta forma se reducirá el riesgo de ataques DoS y DDoS. Puede proteger aún más el host ESXi y las máquinas virtuales si instala firewalls de software en los extremos delanteros y traseros de la DMZ. Por último, asegúrese de que el host esté detrás de un firewall físico y configure los recursos de almacenamiento en red para que cada uno tenga su propio conmutador virtual.

Usar el protocolo Internet Protocol Security en hosts ESXi

El protocolo Internet Protocol Security (IPsec) protege las comunicaciones de IP que recibe y envía un host. Los hosts ESXi admiten IPsec con IPv6.

Al configurar IPsec en un host ESXi, se habilita la autenticación y el cifrado de paquetes entrantes y salientes. El momento y el modo en que el tráfico de IP se cifra dependen de la configuración de las asociaciones de seguridad del sistema y de las directivas de seguridad.

Una asociación de seguridad determina el modo en que el sistema cifra el tráfico. Al crear una asociación de seguridad, se especifican el origen y el destino, los parámetros de cifrado y un nombre para la asociación de seguridad.

Una directiva de seguridad determina el momento en el que el sistema debe cifrar el tráfico. La directiva de seguridad incluye la información del origen y destino, el protocolo y la dirección del tráfico que se va a cifrar, el modo (transporte o túnel) y la asociación de seguridad que se deben utilizar.

Enumerar las asociaciones de seguridad disponibles en hosts ESXi

ESXi puede proporcionar una lista de todas las asociaciones de seguridad disponibles que pueden usar las directivas de seguridad. La lista incluye tanto las asociaciones de seguridad creadas por el usuario como las asociaciones de seguridad que haya instalado el VMkernel con el intercambio de claves por red.

Puede obtener una lista de las asociaciones de seguridad disponibles usando el comando `esxcli`.

Procedimiento

- En el símbolo del sistema, introduzca el comando **`esxcli network ip ipsec sa list`**.

Resultados

ESXi muestra una lista de todas las asociaciones de seguridad disponibles.

Agregar una asociación de seguridad de IPsec a un host ESXi

Agregue una asociación de seguridad a fin de especificar parámetros de cifrado para el tráfico de IP asociado.

Puede agregar una asociación de seguridad mediante el comando `esxcli`.

Procedimiento

- En el símbolo del sistema, introduzca el comando **`esxcli network ip ipsec sa add`** con una o más de las siguientes opciones.

Opción	Descripción
`--sa-source=` *source address*	Requerido. Especifique la dirección de origen.
`--sa-destination=` *destination address*	Requerido. Especifique la dirección de destino.
`--sa-mode=` *mode*	Requerido. Especifique el modo, ya sea `transport` o `tunnel`.
`--sa-spi=` *security parameter index*	Requerido. Especifique el índice de parámetros de seguridad. El índice de parámetros de seguridad identifica la asociación de seguridad con el host. Debe ser un número hexadecimal con un prefijo 0x. Cada asociación de seguridad que cree debe tener una combinación única de protocolo e índice de parámetros de seguridad.
`--encryption-algorithm=` *encryption algorithm*	Requerido. Especifique el algoritmo de cifrado mediante uno de los siguientes parámetros. ■ `3des-cbc` ■ `aes128-cbc` ■ `null` (no proporciona cifrado)
`--encryption-key=` *encryption key*	Requerido al especificar un algoritmo de cifrado. Especifique la clave de cifrado. Puede introducir claves como texto ASCII o un número hexadecimal con un prefijo 0x.

Opción	Descripción
--integrity-algorithm= *authentication algorithm*	Requerido. Especifique el algoritmo de autenticación, ya sea `hmac-sha1` o `hmac-sha2-256`.
--integrity-key= *authentication key*	Requerido. Especifique la clave de autenticación. Puede introducir claves como texto ASCII o un número hexadecimal con un prefijo 0x.
--sa-name=*name*	Requerido. Proporcione un nombre para la asociación de seguridad.

Ejemplo: Nuevo comando de asociación de seguridad

El siguiente ejemplo contiene saltos de línea adicionales para facilitar la lectura.

```
esxcli network ip ipsec sa add
--sa-source 3ffe:501:ffff:0::a
--sa-destination 3ffe:501:ffff:0001:0000:0000:0000:0001
--sa-mode transport
--sa-spi 0x1000
--encryption-algorithm 3des-cbc
--encryption-key 0x6970763672656164796c6f676f336465736362636f757432
--integrity-algorithm hmac-sha1
--integrity-key 0x6970763672656164796c6f67736861316f757432
--sa-name sa1
```

Quitar una asociación de seguridad de IPsec de un host ESXi

Una asociación de seguridad se puede eliminar usando el comando ESXCLI.

Requisitos previos

Compruebe que la asociación de seguridad que desea utilizar no esté en uso. Si intenta eliminar una asociación de seguridad en uso, la operación de eliminación generará errores.

Procedimiento

- En el símbolo del sistema, introduzca el comando **esxcli network ip ipsec sa remove --sa-name** ***security_association_name***.

Enumerar las directivas de seguridad de IPsec disponibles en un host ESXi

Las directivas de seguridad disponibles se pueden mostrar con el comando ESXCLI.

Procedimiento

- En el símbolo del sistema, introduzca el comando **esxcli network ip ipsec sp list**.

Resultados

El host muestra una lista de todas las directivas de seguridad disponibles.

Crear una directiva de seguridad de IPSec en un host ESXi

Cree una directiva de seguridad para determinar cuándo se debe utilizar el conjunto de parámetros de autenticación y cifrado en una asociación de seguridad. Puede agregar una directiva de seguridad mediante el comando ESXCLI.

Requisitos previos

Antes de crear una directiva de seguridad, agregue una asociación de seguridad con los parámetros de autenticación y cifrado adecuados, tal como se describe en Agregar una asociación de seguridad de IPsec a un host ESXi.

Procedimiento

- En el símbolo del sistema, introduzca el comando **esxcli network ip ipsec sp add** con una o más de las siguientes opciones.

Opción	Descripción
--sp-source= *source address*	Requerido. Especifique la dirección IP de origen y la longitud del prefijo.
--sp-destination= *destination address*	Requerido. Especifique la dirección de destino y la longitud del prefijo.
--source-port= *port*	Requerido. Especifique el puerto de origen. El puerto de origen debe ser un número entre 0 y 65535.
--destination-port= *port*	Requerido. Especifique el puerto de destino. El puerto de origen debe ser un número entre 0 y 65535.
--upper-layer-protocol= *protocol*	Especifique el protocolo de capa superior mediante uno de los siguientes parámetros. ■ `tcp` ■ `udp` ■ `icmp6` ■ `any`
--flow-direction= *direction*	Especifique la dirección en la que desea supervisar el tráfico mediante `in` o `out`.
--action= *action*	Utilice los siguientes parámetros para especificar la acción que se debe realizar cuando se encuentra tráfico con los parámetros especificados. ■ `none`: no realice ninguna acción. ■ `discard`: no permita la entrada o salida de datos. ■ `ipsec`: utilice la información de autenticación y cifrado proporcionada en la asociación de seguridad para determinar si los datos provienen de un origen confiable.
--sp-mode= *mode*	Especifique el modo, ya sea `tunnel` o `transport`.
--sa-name=*security association name*	Requerido. Proporcione el nombre de la asociación de seguridad para la directiva de seguridad que se va a utilizar.
--sp-name=*name*	Requerido. Proporcione un nombre para la directiva de seguridad.

Ejemplo: Nuevo comando de directiva de seguridad

En el siguiente ejemplo se incluyen saltos de línea adicionales para facilitar la lectura.

```
esxcli network ip ipsec add
--sp-source=2001:db8:1::/64
--sp-destination=2002:db8:1::/64
--source-port=23
--destination-port=25
--upper-layer-protocol=tcp
--flow-direction=out
--action=ipsec
--sp-mode=transport
--sa-name=sa1
--sp-name=sp1
```

Quitar una directiva de seguridad de IPsec de un host ESXi

Una directiva de seguridad se puede eliminar del host ESXi usando el comando ESXCLI.

Requisitos previos

Compruebe que la directiva de seguridad que desea utilizar no esté en uso. Si intenta eliminar una directiva de seguridad en uso, la operación de eliminación generará errores.

Procedimiento

- En el símbolo del sistema, introduzca el comando **esxcli network ip ipsec sp remove --sa-name *security policy name***.

  Para eliminar todas las directivas de seguridad, introduzca el comando **esxcli network ip ipsec sp remove --remove-all**.

Garantizar una configuración de SNMP adecuada en los hosts ESXi

Si SNMP no se configura correctamente, puede enviarse información de supervisión a un host malicioso. El host malicioso puede usar esta información para planificar un ataque.

ESXi incluye un agente de SNMP que puede enviar notificaciones (capturas e informes) y recibir solicitudes `GET`, `GETBULK` y `GETNEXT`. SNMP no está activado de forma predeterminada. SNMP debe configurarse en cada host ESXi. Puede usar ESXCLI, PowerCLI o vSphere Web Services SDK para la configuración.

Consulte la documentación *Supervisión y rendimiento de vSphere* para obtener información detallada sobre la configuración de SNMP, incluido SNMP v3. SNMP v3 proporciona una seguridad más sólida que SNMP v1 o SNMP v2c, que incluye cifrado y autenticación de claves. Consulte *Referencia de ESXCLI* para obtener más información sobre las opciones del comando `esxcli system snmp`.

Procedimiento

1 Para determinar si se utiliza SNMP, ejecute el siguiente comando.

```
esxcli system snmp get
```

2 Para activar SNMP, ejecute el siguiente comando.

```
esxcli system snmp set --enable true
```

3 Para desactivar SNMP, ejecute el siguiente comando.

```
esxcli system snmp set --enable false
```

Prácticas recomendadas de seguridad de redes de vSphere

Seguir las prácticas recomendadas de seguridad de redes permite garantizar la integridad de la implementación de vSphere.

Recomendaciones generales sobre seguridad de redes de vSphere

El primer paso para proteger el entorno de las redes de vSphere es seguir las recomendaciones generales sobre seguridad de red. A continuación, puede pasar a áreas especiales, como la protección de la red con firewalls o IPsec.

Recomendaciones para proteger un entorno de redes de vSphere

- El protocolo de árbol de expansión (Spanning Tree Protocol, STP) detecta cuándo se van a formar bucles en la topología de la red e impide que suceda. Los conmutadores virtuales de VMware evitan los bucles de otras maneras, pero no admiten el protocolo STP directamente. Cuando se producen cambios en la topología de la red, se necesita un tiempo (entre 30 y 50 segundos) para que la red reconozca la topología. Durante ese tiempo, no se permite que el tráfico pase. Para evitar estos problemas, los proveedores de red han creado funciones para que los puertos de conmutador sigan reenviando el tráfico. Para obtener más información, consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/1003804. Consulte la documentación del proveedor de red para conocer las configuraciones de red y de hardware de red adecuadas.
- Asegúrese de que el tráfico de Netflow de un conmutador virtual distribuido se envíe solamente a direcciones IP de recopiladores autorizados. Las exportaciones de Netflow no están cifradas y pueden contener información sobre la red virtual. Con esta información aumenta la posibilidad de que los atacantes puedan ver y capturar información confidencial. Si se necesita una exportación de Netflow, compruebe que todas las direcciones IP de destino de Netflow sean correctas.
- Use los controles de acceso basado en funciones para asegurarse de que solo los administradores autorizados tengan acceso a los componentes de redes virtuales. Por ejemplo, se debe otorgar a los administradores de máquinas virtuales acceso solo a los grupos de puertos en los que residen sus máquinas virtuales. Otorgue a los administradores

de red acceso a todos los componentes de redes virtuales, pero no acceso a las máquinas virtuales. Si se limita el acceso, se reduce el riesgo de una configuración incorrecta, ya sea accidental o malintencionada, y se aplican los conceptos de seguridad clave de división de tareas y privilegios mínimos.

- Asegúrese de que los grupos de puertos no estén configurados con el valor de la VLAN nativa. A menudo, los conmutadores físicos se configuran con una VLAN nativa y esa VLAN nativa suele ser VLAN 1 de forma predeterminada. ESXi no tiene una VLAN nativa. Las tramas con VLAN especificadas en el grupo de puertos tienen una etiqueta, pero las tramas con VLAN no especificadas en el grupo de puertos no están etiquetadas. Esta situación puede generar un problema porque las máquinas virtuales que se etiquetan con un 1 terminan perteneciendo a una VLAN nativa del conmutador físico.

  Por ejemplo, las tramas de la VLAN 1 de un conmutador físico de Cisco no tienen etiquetas porque la VLAN 1 es la VLAN nativa de ese conmutador físico. No obstante, los marcos del host ESXi que están especificados como VLAN 1 se etiquetan con un 1. Como resultado, el tráfico del host ESXi que está destinado a la VLAN nativa no se enruta correctamente porque está etiquetado con un 1 en lugar de no tener etiqueta. El tráfico del conmutador físico que viene de la VLAN nativa no es visible porque no está etiquetado. Si el grupo de puertos del conmutador virtual de ESXi usa el identificador de la VLAN nativa, el tráfico proveniente de las máquinas virtuales de ese puerto no será visible para la VLAN nativa del conmutador, ya que este último espera tráfico sin etiquetas.

- Asegúrese de que los grupos de puertos no estén configurados con los valores de la VLAN reservados para los conmutadores físicos ascendentes. Los conmutadores físicos reservan ciertos identificadores de VLAN para fines internos y generalmente no permiten el tráfico configurado con estos valores. Por ejemplo, los conmutadores Cisco Catalyst generalmente reservan las VLAN 1001-1024 y 4094. El uso de una VLAN reservada puede provocar la denegación de servicio en la red.

- Asegúrese de que los grupos de puertos no estén configurados con la VLAN 4095, con excepción del etiquetado de invitado virtual (VGT). Al configurar un grupo de puertos con la VLAN 4095, se activa el modo de VGT. En este modo, el conmutador virtual pasa todas las tramas de red a la máquina virtual sin modificar las etiquetas de la VLAN, y deja que la máquina virtual se encargue de ellas.

- Restrinja las anulaciones de la configuración de nivel de puerto de un conmutador virtual distribuido. Las anulaciones de la configuración de nivel de puerto están desactivadas de forma predeterminada. Cuando se activan las anulaciones, se puede usar una configuración de seguridad diferente para una máquina virtual y para el nivel de grupo de puertos. Algunas máquinas virtuales requieren una configuración única, pero la supervisión es fundamental. Si las anulaciones no se supervisan, cualquiera que tenga acceso a una máquina virtual con una configuración de conmutador virtual distribuido poco segura puede intentar aprovecharse de dicho acceso.

- Asegúrese de que el tráfico reflejado del conmutador virtual distribuido se envíe solo a los puertos o las VLAN de recopiladores autorizados. vSphere Distributed Switch puede reflejar el tráfico de un puerto a otro para permitir que los dispositivos de captura de paquetes

recopilen flujos de tráfico específicos. La funcionalidad de creación de reflejo de puertos envía una copia de todo el tráfico especificado en formato no cifrado. El tráfico reflejado contiene todos los datos en los paquetes capturados, por lo que tales datos pueden verse afectados por completo si se envían a una dirección incorrecta. Si se requiere la creación de reflejo del puerto, verifique que la VLAN de destino del puerto reflejado, el puerto y los identificadores de vínculo superior sean correctos.

Etiquetar componentes de redes de vSphere

La identificación de los diversos componentes de la arquitectura de redes de vSphere es esencial y permite garantizar que no se introduzcan errores a medida que se expande la red.

Siga estas prácticas recomendadas:

- Asegúrese de que los grupos de puertos se configuren con una etiqueta de red clara. Estas etiquetas actúan como un descriptor de funciones del grupo de puertos y permiten identificar la función de cada grupo de puertos a medida que se incrementa la complejidad de la red.
- Asegúrese de que cada vSphere Distributed Switch contenga una etiqueta de red clara donde se indique la función o la subred IP de ese conmutador. Esta etiqueta actúa como un descriptor de funciones para el conmutador, al igual que el nombre de host requerido para los conmutadores físicos. Por ejemplo, se puede etiquetar el conmutador como interno para indicar que es para las redes internas. No se puede cambiar la etiqueta de un conmutador virtual estándar.

Documentación y verificación del entorno VLAN de vSphere

Compruebe el entorno de VLAN regularmente para evitar futuros problemas. Documente en detalle el entorno de VLAN y asegúrese de que los identificadores de VLAN se utilicen una sola vez. La documentación puede ayudar a solucionar problemas y resulta fundamental para expandir el entorno.

Procedimiento

1. Asegúrese de que todos los identificadores de vSwitch y VLAN estén documentados detalladamente.

   Si utiliza un etiquetado de VLAN en un conmutador virtual, los identificadores deben coincidir con los identificadores de los conmutadores ascendentes con reconocimiento de VLAN. Si no se hace un seguimiento completo de los identificadores de VLAN, la reutilización de identificadores por error puede producir tráfico entre las máquinas virtuales y físicas inadecuadas. De modo similar, si los identificadores de VLAN son incorrectos o faltan, puede bloquearse el tráfico entre las máquinas físicas y virtuales en los lugares donde el tráfico debiera circular.

2. Compruebe que los identificadores de VLAN de todos los grupos de puertos virtuales distribuidos (instancias dvPortgroup) estén documentados detalladamente.

   Si utiliza un etiquetado de VLAN en un dvPortgroup, los identificadores deben coincidir con los identificador de los conmutadores ascendentes externos con reconocimiento de VLAN.

Si no se hace un seguimiento completo de los identificadores de VLAN, la reutilización de identificadores por error puede producir tráfico entre las máquinas virtuales y físicas inadecuadas. De modo similar, si los identificadores de VLAN son incorrectos o faltan, puede bloquearse el tráfico entre las máquinas físicas y virtuales en los lugares donde el tráfico debiera circular.

3 Compruebe que los identificadores de VLAN privada de todos los conmutadores virtuales distribuidos estén documentados detalladamente.

   Las VLAN privadas (PVLAN) de los conmutadores virtuales distribuidos requieren identificadores de VLAN principales y secundarios. Estos identificadores deben coincidir con los identificadores de los conmutadores ascendentes externos con reconocimiento de PVLAN. Si no se hace un seguimiento completo de los identificadores de VLAN, la reutilización de identificadores por error puede producir tráfico entre las máquinas virtuales y físicas inadecuadas. De modo similar, si los identificadores de PVLAN son incorrectos o faltan, puede bloquearse el tráfico entre las máquinas físicas y virtuales en los lugares donde el tráfico debiera circular.

4 Compruebe que los enlaces troncales de VLAN estén conectados únicamente a los puertos de conmutadores físicos que funcionan como enlaces troncales.

   Cuando conecte un conmutador virtual a un puerto troncal de VLAN, debe configurar correctamente tanto el conmutador virtual como el físico en el puerto de vínculo superior. Si el conmutador físico no está configurado adecuadamente, se reenvían las tramas con el encabezado VLAN 802.1q a un conmutador que no espera esa llegada.

Adoptar prácticas de aislamiento de red en vSphere

Las prácticas de aislamiento de red refuerzan la seguridad de la red en su entorno de vSphere.

Aislar la red de administración de vSphere

La red de administración de vSphere proporciona acceso a la interfaz de administración de vSphere en cada componente. Los servicios que se ejecutan en la interfaz de administración ofrecen una oportunidad para que un atacante obtenga acceso con privilegios a los sistemas. Los ataques remotos suelen comenzar al obtener acceso a esta red. Si un atacante obtiene acceso a la red de administración, significa que ha dado un gran paso para seguir obteniendo acceso no autorizado.

Para lograr un control estricto del acceso a la red de administración, protéjalo con el nivel de seguridad de la máquina virtual más segura que se ejecuta en un host o clúster de ESXi. Más allá del nivel de restricción que tenga la red de administración, los administradores deben acceder a ella para configurar los hosts ESXi y el sistema vCenter Server.

Coloque el grupo de puertos de administración de vSphere en una VLAN dedicada de un conmutador estándar común. El tráfico (de máquinas virtuales) de producción puede compartir el conmutador estándar si las máquinas virtuales de producción no utilizan la VLAN del grupo de puertos de administración de vSphere.

Compruebe que el segmento de red no esté enrutado, excepto en las redes en las que haya otras entidades relacionadas con la administración. Enrutar un segmento de red podría tener sentido para vSphere Replication. En particular, asegúrese de que el tráfico de las máquinas virtuales de producción no se pueda enrutar a esta red.

Para lograr un control estricto del acceso a la funcionalidad de administración, use uno de los métodos siguientes.

- Para acceder a la red de administración en entornos especialmente confidenciales, configure una puerta de enlace controlada u otro método controlado. Por ejemplo, requiera que los administradores se conecten a la red de administración a través de una VPN. Conceda acceso a la red de administración solo a los administradores de confianza.
- Configure hosts bastión que ejecuten clientes de administración.

Aislar el tráfico de almacenamiento

Compruebe que el tráfico de almacenamiento basado en IP esté aislado. El almacenamiento basado en IP incluye iSCSI y NFS. Las máquinas virtuales pueden compartir conmutadores virtuales y VLAN con configuraciones de almacenamiento basadas en IP. Este tipo de configuración puede exponer el tráfico de almacenamiento basado en IP a usuarios de máquinas virtuales no autorizados.

El almacenamiento basado en IP no suele estar cifrado. Cualquier persona que tenga acceso a esta red puede ver el tráfico de almacenamiento basado en IP. Para impedir que usuarios no autorizados vean el tráfico de almacenamiento basado en IP, separe lógicamente el tráfico de red de almacenamiento basado en IP del tráfico de producción. Configure los adaptadores de almacenamiento basado en IP en VLAN distintas o segmentos de red de la red de administración VMkernel para restringir la visualización del tráfico a usuarios no autorizados.

Aislar el tráfico de vMotion

La información de migración de vMotion se transmite en texto sin formato. Cualquiera que tenga acceso a la red puede ver la información que pasa por ella. Los posibles atacantes pueden interceptar el tráfico de vMotion para obtener el contenido de memoria de una máquina virtual. También pueden preparar un ataque de MITM en el que el contenido se modifica durante la migración.

Separe el tráfico de vMotion del tráfico de producción en una red aislada. Configure la red para que no se pueda enrutar, es decir, asegúrese de que no haya un enrutador de Capa 3 expandiendo esta u otras redes, a fin de restringir el acceso exterior a esta red.

Use una VLAN dedicada en un conmutador estándar común para el grupo de puertos de vMotion. El tráfico (de máquinas virtuales) de producción puede usar el mismo conmutador estándar si las máquinas virtuales de producción no utilizan la VLAN del grupo de puertos de vMotion.

Aislar el tráfico de vSAN

Al configurar la red de vSAN, aísle el tráfico de vSAN en su propio segmento de red de capa 2. Puede realizar este aislamiento mediante conmutadores o puertos dedicados o a través de una VLAN.

Usar conmutadores virtuales con vSphere Network Appliance API solo cuando es necesario

No configure el host para que envíe información de red a una máquina virtual a menos que esté utilizando productos que usan vSphere Network Appliance API (DvFilter). Si vSphere Network Appliance API está habilitado, un atacante puede intentar conectar una máquina virtual al filtro. Esta conexión puede abrir el acceso a la red de otras máquinas virtuales del host.

Si utiliza un producto que usa esta API, compruebe que el host esté configurado correctamente. Consulte las secciones sobre DvFilter en la documentación de *Desarrollo e implementación de soluciones de vSphere, vServices y agentes de ESX*. Si el host está configurado para usar la API, compruebe que el valor del parámetro `Net.DVFilterBindIpAddress` coincida con el producto que usa la API.

Procedimiento

1 Desplácese hasta el host en el inventario de vSphere Client.

2 Haga clic en **Configurar**.

3 En Sistema, haga clic en **Configuración avanzada del sistema**.

4 Desplácese hacia abajo hasta `Net.DVFilterBindIpAddress` y compruebe que el parámetro tenga un valor vacío.

   El orden de los parámetros no es estrictamente alfabético. Escriba **`DVFilter`** en el cuadro de texto Filtrar para mostrar todos los parámetros relacionados.

5 Compruebe la configuración.

   - Si no utiliza la configuración de DvFilter, asegúrese de que el valor esté en blanco.
   - Si está utilizando la configuración de DvFilter, asegúrese de que el valor del parámetro sea correcto. El valor debe coincidir con el valor del producto que usa el DvFilter.

Prácticas recomendadas relacionadas con varios componentes de vSphere

14

Algunas prácticas recomendadas de seguridad, como la configuración de PTP o NTP en el entorno, tienen efecto en más de un componente de vSphere. Tenga en cuenta estas recomendaciones al configurar el entorno.

Consulte Capítulo 3 Proteger hosts ESXi y Capítulo 5 Proteger máquinas virtuales para obtener información relacionada.

Lea los siguientes temas a continuación:

Sincronizar los relojes en la red de vSphere

Compruebe que todos los componentes de la red de vSphere tengan sus relojes sincronizados. Si los relojes en las máquinas físicas de la red de vSphere no están sincronizados, los certificados SSL y los tokens SAML, que están sujetos a limitaciones temporales, pueden no reconocerse como válidos en las comunicaciones entre máquinas de la red.

Los relojes que no están sincronizados pueden ocasionar problemas de autenticación que, a su vez, pueden provocar errores en la instalación o evitar que se inicie el servicio `vmware-vpxd` de vCenter Server.

Las incoherencias de hora en vSphere pueden hacer que el primer arranque de un componente en su entorno falle en los diferentes servicios según la ubicación en el entorno donde la hora no sea precisa y el momento en el que se sincronice la hora. Normalmente, los problemas se producen cuando el host ESXi de destino para la instancia de vCenter Server de destino no está sincronizado con NTP o PTP. De forma similar, se pueden presentar problemas si el dispositivo vCenter Server de destino se migra a un host ESXi establecido en otra hora debido a un DRS completamente automatizado.

Para evitar problemas de sincronización de hora, asegúrese de que lo siguiente sea correcto antes de instalar, migrar o actualizar una instancia vCenter Server.

- El host ESXi de destino donde se desea implementar la instancia de vCenter Server de destino está sincronizado con NTP o PTP.
- El host ESXi donde se ejecuta la instancia de vCenter Server de origen está sincronizado con NTP o PTP.
- Al actualizar o migrar desde vSphere 6.7 a vSphere 8.0, si la instancia de vCenter Server Appliance está conectada a una instancia externa de Platform Services Controller, asegúrese de que el host ESXi donde se ejecuta la instancia externa de Platform Services Controller esté sincronizado con NTP o PTP.
- Si va a actualizar o migrar desde vSphere 6.7 a vSphere 8.0, compruebe que la instancia de origen de vCenter Server o vCenter Server Appliance y la instancia externa de Platform Services Controller tengan la hora correcta.

Verifique que todos los equipos host de Windows en los que se ejecuta vCenter Server estén sincronizados con el servidor de tiempo de red (NTP). Consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/1318.

Para sincronizar los relojes de ESXi con un servidor NTP o PTP, puede usar VMware Host Client. Para obtener información sobre la edición de la configuración de hora de un host ESXi, consulte el tema *Editar la configuración de hora de un host ESXi en VMware Host Client* en la documentación *Administrar un host único de vSphere: VMware Host Client*.

Para obtener información sobre cómo cambiar la configuración de sincronización de hora para vCenter Server, consulte el tema *Configurar la zona horaria y la sincronización de hora del sistema* en la documentación *Configuración de vCenter Server*.

Para obtener información sobre cómo editar la configuración de hora de un host mediante vSphere Client, consulte el tema *Editar la configuración de hora para un host* en la documentación *Administrar vCenter Server y hosts*.

Qué leer a continuación

- Sincronización de los relojes de ESXi con un servidor horario de red

  Antes de instalar vCenter Server, asegúrese que todas las máquinas de la red de vSphere tengan los relojes sincronizados.

- Configurar la sincronización de hora en vCenter Server

  Puede cambiar la configuración de sincronización de hora en vCenter Server tras la implementación.

Sincronización de los relojes de ESXi con un servidor horario de red

Antes de instalar vCenter Server, asegúrese que todas las máquinas de la red de vSphere tengan los relojes sincronizados.

Esta tarea explica cómo configurar NTP desde VMware Host Client.

Procedimiento

1 Inicie VMware Host Client y conéctese al host ESXi.

2 Haga clic en **Administrar**.

3 En **Sistema**, haga clic en **Hora y fecha** y, a continuación, en **Editar configuración**.

4 Seleccione **Usar protocolo de hora de red (Habilitar el cliente NTP)**.

5 En el cuadro de texto Servidores NTP, introduzca la dirección IP o el nombre de dominio completo de uno o más servidores NTP con los que se realizará la sincronización.

6 En el menú desplegable **Directiva de inicio del servicio NTP**, seleccione **Iniciar y detener con el host**.

7 Haga clic en **Guardar**.

   El host se sincroniza con el servidor NTP.

Configurar la sincronización de hora en vCenter Server

Puede cambiar la configuración de sincronización de hora en vCenter Server tras la implementación.

Cuando implementa vCenter Server, puede decidir que el método de sincronización de hora sea mediante un servidor NTP o a través de VMware Tools. En caso de que la configuración de hora de la red de vSphere cambie, puede editar vCenter Server y configurar la sincronización horaria mediante los comandos del shell del dispositivo.

Cuando habilita la sincronización horaria periódica, VMware Tools configura la hora del sistema operativo invitado para que sea la misma que la hora del host.

Una vez que se sincroniza la hora, VMware Tools comprueba cada un minuto si los relojes del sistema operativo invitado y el host aún coinciden. Si no lo hacen, el reloj del sistema operativo invitado se sincroniza para que coincida con el reloj del host.

El software de sincronización de hora nativo, como el protocolo de hora de red (Network Time Protocol, NTP), suele ser más preciso que la sincronización horaria periódica de VMware Tools y, por lo tanto, es el método preferido. En vCenter Server, solo puede utilizar un modo de sincronización de hora periódica. Si decide utilizar software de sincronización de hora nativo, se desactiva la sincronización de hora periódica de VMware Tools en vCenter Server.

Usar la sincronización de hora de VMware Tools

Puede configurar vCenter Server para utilizar la sincronización de hora de VMware Tools.

Procedimiento

1 Acceda al shell del dispositivo e inicie sesión como usuario que tiene la función de administrador o superadministrador.

   El usuario predeterminado con la función de superadministrador es root.

2 Ejecute el comando para habilitar la sincronización de hora de VMware Tools.

```
timesync.set --mode host
```

3 (opcional) Ejecute el comando para comprobar que la sincronización de hora de VMware Tools se aplicó correctamente.

```
timesync.get
```

El comando devuelve un mensaje donde se indica que la sincronización de hora se encuentra en el modo host.

Resultados

La hora del dispositivo se sincroniza con la hora del host ESXi.

Agregar o reemplazar servidores NTP en la configuración de vCenter Server

Para configurar vCenter Server de modo que utilice la sincronización de hora basada en NTP, debe agregar los servidores NTP a la configuración de vCenter Server.

Procedimiento

1 Acceda al shell del dispositivo e inicie sesión como usuario que tiene la función de administrador o superadministrador.

El usuario predeterminado con la función de superadministrador es root.

2 Agregue servidores NTP a la configuración de vCenter Server mediante la ejecución del siguiente comando `ntp.set`.

```
ntp.set --servers IP-addresses-or-host-names
```

En este comando, *IP-addresses-or-host-names* es una lista separada por comas de direcciones IP o nombres de host de los servidores NTP.

Este comando elimina los servidores NTP actuales (si existe alguno) y agrega los nuevos servidores NTP a la configuración. Si la sincronización de hora se basa en un servidor NTP, el daemon de NTP se reinicia para volver a cargar los nuevos servidores NTP. De lo contrario, este comando reemplaza los servidores NTP actuales en la configuración de NTP por los nuevos servidores NTP que especifique.

3 (opcional) Para comprobar que aplicó correctamente la nueva configuración de NTP, ejecute el siguiente comando.

```
ntp.get
```

El comando devuelve una lista separada con espacios de los servidores configurados para la sincronización de NTP. Si la sincronización de NTP está activada, el comando informa de que el estado de la configuración de NTP es Activado. Si la sincronización de NTP está desactivada, el comando informa de que el estado de la configuración de NTP es Desactivado.

4 (opcional) Para comprobar si se puede acceder al servidor NTP, ejecute el siguiente comando.

```
ntp.test --servers IP-addresses-or-host-names
```

El comando devuelve el estado de los servidores NTP.

Pasos siguientes

Si la sincronización de NTP está desactivada, se puede configurar la sincronización de hora en vCenter Server para que se base en un servidor NTP. Consulte Sincronizar la hora de vCenter Server con un servidor NTP.

Sincronizar la hora de vCenter Server con un servidor NTP

Puede configurar la sincronización de hora en vCenter Server para que se base en un servidor NTP.

Requisitos previos

Establezca uno o más servidores de protocolo de hora de red (Network Time Protocol, NTP) en la configuración de vCenter Server. Consulte Agregar o reemplazar servidores NTP en la configuración de vCenter Server.

Procedimiento

1 Acceda al shell del dispositivo e inicie sesión como usuario que tiene la función de administrador o superadministrador.

   El usuario predeterminado con la función de superadministrador es root.

2 Ejecute el comando para habilitar la sincronización de hora basada en NTP.

```
timesync.set --mode NTP
```

3 (opcional) Ejecute el comando para comprobar que se aplicó correctamente la sincronización de NTP.

```
timesync.get
```

   El comando devuelve que la sincronización de hora se encuentra en el modo NTP.

Prácticas recomendadas de seguridad de almacenamiento

Siga las prácticas recomendadas de seguridad de almacenamiento que indica su proveedor de seguridad de almacenamiento. También puede aprovechar CHAP y Mutual CHAP para proteger el almacenamiento iSCSI, crear máscaras para los recursos de SAN y dividirlos en zonas, y configurar credenciales Kerberos para NFS 4.1.

Consulte además la documentación de *Administrar VMware vSAN*.

Proteger almacenamiento iSCSI

El almacenamiento que se configura en un host puede incluir una o más redes de área de almacenamiento (SAN) que utilizan iSCSI. Cuando se configura iSCSI en un host, se pueden tomar medidas para minimizar los riesgos de seguridad.

iSCSI admite el acceso a los dispositivos SCSI y el intercambio de datos mediante TCP/IP en un puerto de red en lugar de hacerlo a través de una conexión directa con el dispositivo SCSI. Una transacción de iSCSI encapsula bloques de datos SCSI sin formato en registros iSCSI y transmite los datos al dispositivo o el usuario que los solicite.

Las SAN iSCSI admiten el uso eficaz de la infraestructura Ethernet existente para proporcionar acceso a los hosts a los recursos de almacenamiento que pueden compartir dinámicamente. Las SAN iSCSI son una solución de almacenamiento económica para los entornos que dependen de un grupo de almacenamiento común para varios usuarios. Al igual que con cualquier sistema en red, la seguridad de las SAN iSCSI puede verse comprometida debido a infracciones.

Nota Los requisitos y procedimientos para proteger la SAN iSCSI son similares para los adaptadores iSCSI de hardware asociados a los hosts y para iSCSI configurado directamente mediante el host.

Proteger dispositivos de iSCSI

Para proteger los dispositivos de iSCSI, es necesario que el host ESXi o el iniciador puedan autenticarse en el dispositivo de iSCSI o en el destino, siempre que el host intente acceder a datos del LUN de destino.

La autenticación garantiza que el iniciador tenga derecho a acceder a un destino. Conceda este derecho al configurar la autenticación en el dispositivo de iSCSI.

ESXi no admite el protocolo Secure Remote Protocol (SRP) o los métodos de autenticación de clave pública de iSCSI. Kerberos se puede utilizar solo con NFS 4.1.

ESXi admite la autenticación de CHAP y Mutual CHAP. En el documento *Almacenamiento de vSphere* se explica cómo seleccionar el mejor método de autenticación para el dispositivo de iSCSI y cómo configurar CHAP.

Asegúrese de que las contraseñas de CHAP sean únicas. Configure un secreto de autenticación mutua diferente para cada host. Si es posible, configure un secreto diferente para cada cliente que se conecte al host ESXi. Los secretos exclusivos aseguran que un atacante no pueda crear otro host arbitrario y autenticarse en el dispositivo de almacenamiento, incluso si hay un host está en riesgo. Si hay una contraseña compartida y un host comprometido, un atacante podría autenticarse en el dispositivo de almacenamiento.

Proteger una SAN iSCSI

Al planificar la configuración de iSCSI, tome las medidas necesarias para mejorar la seguridad general de la SAN iSCSI. La configuración de iSCSI es tan segura como la red IP, por lo tanto, si aplica estándares de seguridad adecuados al configurar la red, ayuda a proteger el almacenamiento iSCSI.

A continuación, se presentan sugerencias específicas para aplicar estándares de seguridad adecuados.

Proteger datos transmitidos

Uno de los principales riesgos en las SAN iSCSI es que un atacante puede capturar los datos de almacenamiento transmitidos.

Tome medidas adicionales para evitar que los atacantes vean datos de iSCSI con facilidad. Ni el adaptador de iSCSI de hardware ni el iniciador iSCSI de ESXi cifran los datos que transmiten hacia y desde los destinos, lo que hace que los datos sean más vulnerables a ataques de analizadores de protocolos (sniffer).

Si permite que las máquinas virtuales compartan conmutadores estándar y VLAN con la configuración de iSCSI, se corre el riesgo de que algún atacante de máquinas virtuales haga un uso incorrecto del tráfico iSCSI. Para ayudar a garantizar que los intrusos no puedan escuchar transmisiones de iSCSI, asegúrese de que ninguna de las máquinas virtuales pueda ver la red de almacenamiento iSCSI.

Si usa un adaptador de iSCSI de hardware, puede lograr esto comprobando que el adaptador de iSCSI y el adaptador físico de red de ESXi no se conecten accidentalmente fuera del host debido al uso compartido de un conmutador o a algún otro motivo. Si configura iSCSI directamente mediante el host ESXi, podrá lograr esto configurando el almacenamiento iSCSI con un conmutador estándar diferente al que se usa en las máquinas virtuales.

Además de proteger la SAN iSCSI con un conmutador estándar dedicado, puede configurar la SAN iSCSI en su propia VLAN para mejorar el rendimiento y la seguridad. Al colocar la configuración de iSCSI en una VLAN distinta, se garantiza que ningún dispositivo que no sea el adaptador de iSCSI pueda ver transmisiones dentro de la SAN iSCSI. Además, la congestión de la red desde otros orígenes no puede interferir en el tráfico iSCSI.

Proteger los puertos de iSCSI

Al utilizar dispositivos de iSCSI, ESXi no abre ningún puerto que escuche conexiones de red. Esta medida reduce la posibilidad de que un intruso logre entrar a ESXi por los puertos de reserva y tome el control del host. De esta manera, la ejecución de iSCSI no presenta ningún riesgo adicional de seguridad al final de la conexión de ESXi.

Todos los dispositivos de destino iSCSI que se utilicen deben tener uno o más puertos TCP abiertos para escuchar las conexiones de iSCSI. Si existe alguna vulnerabilidad de seguridad en el software del dispositivo iSCSI, los datos pueden estar en riesgo incluso si ESXi funciona correctamente. Para reducir este riesgo, instale todas las revisiones de seguridad que le proporcione el fabricante del equipo de almacenamiento y limite los dispositivos conectados a la red de iSCSI.

Crear máscaras y dividir en zonas para recursos de SAN

Puede utilizar la división en zonas y el enmascaramiento de LUN para segregar la actividad de SAN y restringir el acceso a los dispositivos de almacenamiento.

Puede proteger el acceso al almacenamiento en el entorno de vSphere mediante la división en zonas y el enmascaramiento de LUN con los recursos de SAN. Por ejemplo, puede administrar zonas definidas para pruebas de manera independiente en la SAN para que no interfieran con la actividad de las zonas de producción. De forma similar, puede configurar diferentes zonas para distintos departamentos.

Al configurar zonas, tenga en cuenta los grupos de hosts que estén configurados en el dispositivo SAN.

Las capacidades de división en zonas y de máscaras para cada conmutador SAN y matriz de disco, junto con las herramientas de administración de enmascaramiento de LUN, son específicas del proveedor.

Consulte la documentación del proveedor de SAN y la documentación de *Almacenamiento de vSphere*.

Usar Kerberos para NFS 4.1

Con la versión 4.1 de NFS, ESXi admite el mecanismo de autenticación Kerberos.

El mecanismo RPCSEC_GSS Kerberos es un servicio de autenticación. Permite instalar un cliente de NFS 4.1 en ESXi para probar su identidad en un servidor NFS antes de montar un recurso compartido de NFS. La seguridad Kerberos utiliza criptografía para funcionar en una conexión de red no segura.

La implementación de ESXi de Kerberos para NFS 4.1 proporciona dos modelos de seguridad, krb5 y krb5i, que ofrecen distintos niveles de seguridad.

- Kerberos para autenticación solamente (krb5) admite la comprobación de identidad.
- Kerberos para autenticación e integridad de datos (krb5i), además de la comprobación de identidad, proporciona servicios de integridad de datos. Estos servicios ayudan a proteger el tráfico de NFS para evitar la alteración mediante la comprobación de posibles modificaciones en los paquetes de datos.

Kerberos admite algoritmos de cifrado que evitan que los usuarios no autorizados puedan acceder al tráfico de NFS. El cliente NFS 4.1 en ESXi intenta usar el algoritmo AES256-CTS-HMAC-SHA1-96 o AES128-CTS-HMAC-SHA1-96 para acceder a un recurso compartido en el servidor NAS. Antes de utilizar los almacenes de datos de NFS 4.1, asegúrese de que AES256-CTS-HMAC-SHA1-96 o AES128-CTS-HMAC-SHA1-96 estén habilitados en el servidor NAS.

En la siguiente tabla, se comparan los niveles de seguridad de Kerberos admitidos por ESXi.

Tabla 14-1. Tipos de seguridad de Kerberos

		ESXi 6.0	ESXi 6.5 y versiones posteriores
Kerberos para autenticación solamente (krb5)	Suma de comprobación de integridad para encabezado RPC	Sí con DES	Sí con AES
	Comprobación de integridad para datos de RPC	No	No
Kerberos para autenticación e integridad de datos (krb5i)	Suma de comprobación de integridad para encabezado RPC	Sin krb5i	Sí con AES
	Comprobación de integridad para datos de RPC		Sí con AES

Al utilizar la autenticación Kerberos, se deben tener en cuenta las siguientes consideraciones:

- ESXi utiliza Kerberos con el dominio de Active Directory.
- Como administrador de vSphere, debe especificar credenciales de Active Directory para proporcionar acceso a un usuario de NFS a los almacenes de datos Kerberos de NFS 4.1. Se utiliza un único conjunto de credenciales para acceder a todos los almacenes de datos Kerberos montados en ese host.
- Cuando varios hosts ESXi comparten el almacén de datos NFS 4.1, se deben utilizar las mismas credenciales de Active Directory para todos los hosts que tienen acceso al almacén de datos compartido. Para automatizar el proceso de asignación, establezca el usuario en los perfiles de host y aplique el perfil a todos los hosts ESXi.
- No se pueden usar dos mecanismos de seguridad, AUTH_SYS y Kerberos, para el mismo almacén de datos NFS 4.1 compartido por varios hosts.

Consulte la documentación de *Almacenamiento de vSphere* para obtener instrucciones paso a paso.

Comprobar que está desactivado el envío de datos de rendimiento del host a los invitados

vSphere incluye contadores de rendimiento de las máquinas virtuales en los sistemas operativos Windows con VMware Tools instalado. Los contadores de rendimiento permiten que los propietarios de las máquinas virtuales realicen análisis precisos del rendimiento en el sistema operativo invitado. De forma predeterminada, vSphere no expone la información del host a la máquina virtual invitada.

De forma predeterminada, la capacidad para enviar datos de rendimiento del host a una máquina virtual está desactivada. Esta configuración predeterminada impide que una máquina virtual obtenga información detallada sobre el host físico. Si se produce una infracción de seguridad de la máquina virtual, la configuración no pone a disposición del atacante los datos del host.

Nota El siguiente procedimiento muestra el proceso básico. Considere la posibilidad de utilizar comandos ESXCLI o de VMware PowerCLI para realizar esta tarea en todos los hosts a la vez.

Procedimiento

1. En el sistema ESXi que aloja a la máquina virtual, desplácese hasta el archivo VMX.

   Los archivos de configuración de la máquina virtual están ubicados en el directorio `/vmfs/volumes/`*`datastore`*, donde *datastore* corresponde al nombre del dispositivo de almacenamiento en el que están almacenados los archivos de la máquina virtual.

2. En el archivo VMX, compruebe que se haya establecido el siguiente parámetro.

   ```
   tools.guestlib.enableHostInfo=FALSE
   ```

3. Guarde y cierre el archivo.

Resultados

No se puede recuperar la información de rendimiento del host desde la máquina virtual invitada.

Configurar tiempos de espera de ESXi Shell y vSphere Client

Para evitar que los intrusos utilicen una sesión inactiva, configure tiempos de espera para ESXi Shell y vSphere Client.

Tiempo de espera de ESXi Shell

Para ESXi Shell, puede establecer los siguientes tiempos de espera desde vSphere Client y la interfaz de usuario de la consola directa (DCUI).

Tiempo de espera de disponibilidad

La configuración de tiempo de espera de disponibilidad corresponde a la cantidad de tiempo que puede transcurrir antes de que pueda iniciar sesión tras la activación de ESXi Shell. Una vez que transcurre el período de espera, el servicio se desactiva y los usuarios no pueden iniciar sesión.

Tiempo de espera de inactividad

El tiempo de espera de inactividad corresponde a la cantidad de tiempo que puede transcurrir antes de que se cierren las sesiones interactivas inactivas. Los cambios en el tiempo de espera de inactividad se aplican la próxima vez que un usuario inicia sesión en ESXi Shell. Los cambios no afectan a las sesiones existentes.

Cambiar el tiempo de espera de vSphere Client

De forma predeterminada, las sesiones de vSphere Client finalizan después de 120 minutos. Para cambiar el valor predeterminado:

1 En vSphere Client, desplácese hasta la instancia de vCenter Server.

2 Seleccione la pestaña **Configurar** y, a continuación, seleccione **General** en **Configuración**.

3 Haga clic en **Editar**.

4 Seleccione **Configuración del tiempo de espera**.

5 Introduzca sus opciones y haga clic en **Guardar**.

Configuración de vSphere TLS

15

A partir de la versión 8.0 Update 3, vSphere admite TLS 1.3 y 1.2 mediante el uso de perfiles de TLS. Los perfiles de TLS simplifican el trabajo de administrar los parámetros de TLS y también mejoran la compatibilidad.

vSphere 8.0 Update 3 activa el perfil de TLS predeterminado, denominado COMPATIBLE, en los hosts de ESXi y vCenter Server. El perfil COMPATIBLE admite TLS 1.3 y algunas conexiones de TLS 1.2.

Puede administrar perfiles de TLS en hosts de ESXi mediante vSphere Configuration Profiles o comandos `esxcli`. En los hosts de vCenter Server, puede administrar perfiles de TLS mediante API. Por ejemplo, puede utilizar el Centro para desarrolladores en vSphere Client. Consulte la *Guía de programación de vSphere Automation SDK* y la *Guía de programación de vSphere Automation REST API*.

vCenter Server y Envoy

vCenter Server ejecuta dos servicios de proxy inverso:

- El servicio de proxy inverso de VMware, `rhttpproxy`
- Envoy

Envoy es un proxy de servicio y una instancia de Edge de código abierto. Envoy tiene el puerto 443 y todas las solicitudes entrantes de vCenter Server se enrutan mediante Envoy. `rhttpproxy` funciona como servidor de administración de configuración para Envoy. Como resultado, la configuración de TLS se aplica a `rhttpproxy` que, a su vez, envía la configuración a Envoy.

Cómo vSphere implementa TLS mediante perfiles de TLS

vSphere 8.0 Update 3 implementa TLS 1.3 mediante la agrupación de parámetros, incluidas las versiones de protocolo, los grupos (también denominados curvas) y los cifrados, en un único perfil de TLS. Este perfil de TLS se aplica a todo el sistema. El uso de un único perfil de TLS facilita la sobrecarga administrativa de los hosts. Ya no es necesario configurar parámetros TLS individuales de forma manual, aunque esa capacidad sigue disponible de ser necesario. Los perfiles de TLS también mejoran de manera significativa la compatibilidad. La agrupación de parámetros en perfiles de TLS simplifica el conjunto de soluciones de TLS verificadas de VMware para elegir. En ESXi, los perfiles de TLS se integran con vSphere Configuration Profiles.

Se proporcionan los siguientes perfiles de TLS de ESXi:

- COMPATIBLE: el perfil predeterminado. La asignación exacta de los parámetros de este perfil puede cambiar de una versión a otra, pero se garantiza que el perfil sea compatible con todos los productos y versiones admitidos (versiones N-2 actuales). Es decir, un host de ESXi de la versión N que utiliza el perfil COMPATIBLE puede comunicarse con un host de la versión N-2.
- NIST_2024: un perfil más restrictivo que admite específicamente el estándar NIST 2024. Se garantiza que la asignación exacta de parámetros de este perfil cumpla con el estándar NIST 2024 en todas las versiones. Se garantiza que este perfil solo sea compatible con las versiones actuales o más recientes, y no con versiones anteriores.
- MANUAL: utilice este perfil para crear y probar una configuración ad hoc en la que proporcione de forma manual los parámetros de TLS. No se garantiza que un perfil MANUAL funcione sin errores. Debe probar un perfil MANUAL, incluidas las actualizaciones de software. Si elige utilizar el perfil MANUAL, el comportamiento del sistema primero se establece de forma predeterminada como el perfil seleccionado antes (COMPATIBLE o NIST_2024) y se mantiene como tal hasta que usted realice cambios. Debe utilizar comandos `esxcli` para administrar el perfil de TLS MANUAL. Consulte el texto de ayuda que se incluye con `esxcli` para obtener más información sobre cómo cambiar los parámetros en un perfil de TLS MANUAL.

Durante la configuración del perfil de TLS al estado deseado, debe reiniciar el host de ESXi o corregir el clúster de vLCM en el que reside el host de ESXi para aplicar los cambios.

En las siguientes tablas, se muestran los detalles de los perfiles de TLS para ESXi y vCenter Server en vSphere 8.0 Update 3. En la columna Lista de cifrados, se muestran los cifrados de TLS para TLS 1.2 y los protocolos inferiores. En la columna Conjuntos de cifrados, se muestran los cifrados del protocolo de TLS 1.3.

Tabla 15-1. Perfiles de TLS 1.3 de ESXi

Nombre del perfil de TLS	Versiones del protocolo de TLS	Lista de cifrados	Conjuntos de claves de cifrado	Curvas	¿VMware es compatible?
COMPATIBLE	TLS 1.3 y TLS 1.2	ECDHE+AESGCM:ECDHE+AES	TLS_AES_256_GCM_SHA384; TLS_AES_128_GCM_SHA256	prime256v1:secp384r1:secp521r1	Sí
NIST_2024	TLS 1.3 y TLS 1.2	ECDHE+AESGCM	TLS_AES_256_GCM_SHA384; TLS_AES_128_GCM_SHA256	prime256v1:secp384r1:secp521r1	Sí
MANUAL	Cualquiera	Cualquiera	Cualquiera	Cualquiera	No

Notas:

- Las opciones de configuración admitidas (protocolos, lista de cifrados, conjuntos de cifrados y curvas) representan lo que se admite como máximo.

- El perfil de NIST_2024 solo se aplica a las conexiones entrantes.
- El módulo criptográfico BoringSSL utilizado en vSphere 8.0 Update 3 aún no alcanzó la certificación de FIPS para el uso de TLS 1.3. Como resultado, tanto en ESXi como en vCenter Server, el puerto 443 (proxy inverso) se comunica mediante TLS 1.2. Los perfiles de TLS COMPATIBLE y NIST_2024 no utilizan TLS 1.3 que no sea FIPS.

Se proporcionan los siguientes perfiles de TLS 1.3 de vCenter Server:

- COMPATIBLE: el perfil predeterminado. La asignación exacta de los parámetros de este perfil puede cambiar de una versión a otra, pero se garantiza que el perfil sea compatible con todos los productos y versiones admitidos (versiones N-2 actuales).
- NIST_2024: un perfil más restrictivo que admite específicamente el estándar NIST 2024. Se garantiza que la asignación exacta de parámetros de este perfil cumpla con el estándar NIST 2024 en todas las versiones. Se garantiza que este perfil solo sea compatible con las versiones actuales o más recientes, y no con versiones anteriores.
- COMPATIBLE-NON-FIPS: un perfil modificado que permite una conexión de TLS 1.3 que no es FIPS desde el proxy de Envoy. FIPS no está habilitado.

Tabla 15-2. Perfiles de TLS 1.3 de vCenter Server

Nombre del perfil de TLS	Versiones del protocolo de TLS	Conjuntos de claves de cifrado	Curvas	¿FIPS está habilitado?	¿VMware es compatible?
COMPATIBLE	TLS 1.3	TLS_AES_256_GCM_SHA384; TLS_AES_128_GCM_SHA256	prime256v1:secp384r1:secp521r1	Sí	Sí
	TLS 1.2	ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES128-GCM-SHA256 AES256-GCM-SHA384 AES128-GCM-SHA256 ECDHE-RSA-AES256-SHA ECDHE-RSA-AES128-SHA ECDHE-ECDSA-AES256-SHA ECDHE-ECDSA-AES128-SHA AES256-SHA AES128-SHA			
NIST_2024	TLS 1.3	TLS_AES_256_GCM_SHA384 TLS_AES_128_GCM_SHA256	prime256v1:secp384r1:secp521r1	Sí	Sí
	TLS 1.2	ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES128-GCM-SHA256			

Tabla 15-2. Perfiles de TLS 1.3 de vCenter Server (continuación)

Nombre del perfil de TLS	Versiones del protocolo de TLS	Conjuntos de claves de cifrado	Curvas	¿FIPS está habilitado?	¿VMware es compatible ?
COMPATIBLE-NON-FIPS	TLS 1.3	TLS_AES_256_GCM_SHA384 TLS_AES_128_GCM_SHA256	prime256v1:secp384r1:secp521r1	No	Sí
	TLS 1.2	ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES128-GCM-SHA256 AES256-GCM-SHA384 AES128-GCM-SHA256 ECDHE-RSA-AES256-SHA ECDHE-RSA-AES128-SHA ECDHE-ECDSA-AES256-SHA ECDHE-ECDSA-AES128-SHA AES256-SHA AES128-SHA			

Conexiones de TLS, entrantes y salientes en ESXi y vCenter Server

ESXi 8.0 Update 3 admite TLS 1.3 en las conexiones entrantes (servidor) y salientes (cliente). Las conexiones entrantes (servidor) de ESXi son las más prioritarias y en ellas se aplica el perfil NIST_2024 más restrictivo.

Para obtener ESXi, puede utilizar las opciones de configuración COMPATIBLE, NIST_2024 y MANUAL en las conexiones entrantes (servidor). Puede utilizar las opciones de configuración COMPATIBLE y MANUAL en las conexiones salientes (cliente).

Los perfiles de TLS de vCenter Server aplican su configuración a las conexiones entrantes y salientes.

Algunos servicios de vSphere exponen puertos que aceptan conexiones de TLS, mientras que la mayoría de los servicios utilizan el proxy inverso. Todas las conexiones entrantes aceptan TLS 1.2 y TLS 1.3 de forma predeterminada. En este momento, el puerto 443 (proxy inverso) tiene TLS 1.3 deshabilitado y se comunica mediante TLS 1.2. Las conexiones salientes admiten TLS 1.2 y TLS 1.3. Para obtener más información, consulte TLS 1.3 en el puerto 443 en ESXi y FIPS.

Administración del ciclo de vida y TLS

La actualización o la migración de un host de ESXi o un host de vCenter Server a la versión 8.0 Update 3 habilita el perfil de TLS COMPATIBLE de forma predeterminada. vSphere 8.0 Update 3 admite TLS 1.3 y TLS 1.2 para la interoperabilidad mínima de forma inmediata. En el futuro, la actualización a una versión posterior de ESXi o vCenter Server mantendrá el perfil de TLS actual en uso siempre que no se haya retirado dicho perfil.

Al actualizar a una versión nueva, como práctica recomendada, primero establezca el perfil de TLS como COMPATIBLE.

Si realiza ediciones en el nivel de servicio local antes de actualizar a vSphere 8.0 Update 3 después de la actualización, se asignará el perfil COMPATIBLE al host, el cual no refleja dichos cambios. Para que el host refleje esos cambios, utilice el perfil MANUAL. Consulte Cambiar el perfil de TLS de un host ESXi mediante vSphere Client o Cambiar el perfil de TLS de un host ESXi mediante la CLI.

Advertencia No se garantiza que el perfil de TLS MANUAL funcione sin errores en todas las actualizaciones. Debe comprobar que un perfil de TLS MANUAL editado funcione de una versión a otra, o cambiar al perfil de TLS COMPATIBLE.

TLS 1.3 en el puerto 443 en ESXi y FIPS

En este momento, vSphere deshabilita TLS 1.3 en el puerto 443. La versión del módulo criptográfico Boring SSL utilizada en vSphere 8.0 Update 3 no cuenta con certificación de FIPS para TLS 1.3. Cuando se utiliza el perfil de TLS COMPATIBLE o NIST_2024, todos los puertos excepto el 443 se comunican mediante TLS 1.3. Por ahora, debido a este problema, el puerto 443 utiliza TLS 1.2.

Para habilitar TLS 1.3 que no es FIPS en el puerto 443, consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/92473.

Lea los siguientes temas a continuación:

Administrar TLS de vSphere

A partir de vSphere 8.0 Update 3 puede administrar perfiles de TLS para ESXi mediante vSphere Client, los comandos `esxcli` o las API. En vCenter Server, los perfiles de TLS se administran mediante las API.

Si utiliza vSphere Configuration Profiles, puede administrar la configuración de TLS para los hosts de ESXi en el nivel de clúster de vLCM. Puede cambiar la configuración de TLS para el clúster y corregir el clúster con esta nueva configuración. Para obtener más información, consulte el capítulo sobre la administración de vSphere Configuration Profiles en la documentación de *Administración del ciclo de vida de hosts y clústeres*.

Para hosts ESXi independientes y clústeres que no sean de vLCM, debe administrar el perfil de TLS mediante comandos `esxcli`. Consulte la documentación de *Conceptos y ejemplos de ESXCLI* y la ayuda en línea de `esxcli`.

En este momento, solo puede administrar perfiles de TLS de vCenter Server mediante las API. Consulte la *Guía de programación de vSphere Automation SDK* y la *Guía de programación de vSphere Automation REST API*.

Ver el perfil de TLS de un host ESXi mediante el vSphere Client

Puede utilizar el vSphere Client para ver el perfil de TLS de un host ESXi que forma parte de un clúster de vLCM.

En vSphere Configuration Profiles, los ajustes que no están configurados explícitamente utilizan los valores predeterminados del perfil adecuado. Para los perfiles TLS, el valor predeterminado es COMPATIBLE.

Para ver el perfil de TLS de un host ESXi de un clúster independiente o que no sea vLCM, consulte Ver el perfil de TLS de un host ESXi mediante la CLI.

Requisitos previos

Habilitó vSphere Configuration Profiles y creó una configuración de borrador para el clúster. Consulte la documentación de *Administración del ciclo de vida de hosts y clústeres*.

Procedimiento

1 En vSphere Client, desplácese hasta el clúster vLCM que administre con una sola imagen.

2 En la pestaña **Configurar**, haga clic en **Estado deseado > Configuración**.

3 En la pestaña **Configuración**, haga clic en **sistema**.

4 Haga clic en **tls_client** o **tls_server** para ver qué perfil de TLS está definido en el documento de configuración actual deseado.

Ver el perfil de TLS de un host ESXi mediante la CLI

Puede usar la CLI para ver el perfil de TLS configurado actualmente de un host ESXi.

Para hosts ESXi independientes y clústeres que no sean de vLCM, debe administrar el perfil de TLS mediante comandos `esxcli`. Para obtener más información, consulte *Referencia de ESXCLI*. Para los hosts ESXi en un clúster de vLCM, puede utilizar vSphere Configuration Profiles o los comandos `esxcli`.

Requisitos previos

Habilite SSH o ESXi Shell en el host ESXi.

Procedimiento

1 Conéctese al host ESXi.

Puede usar SSH o ESXi Shell.

2 Para ver el perfil de TLS configurado actualmente, ejecute el siguiente comando.

```
esxcli system tls [client | server] get
```

3 Para ver los parámetros en el perfil de TLS configurado actualmente, ejecute el siguiente comando:

```
esxcli system tls [client | server] get --show-profile-defaults
```

Cambiar el perfil de TLS de un host ESXi mediante vSphere Client

Puede cambiar el perfil de TLS de un host ESXi. El perfil de TLS predeterminado es COMPATIBLE.

Requisitos previos

Habilitó vSphere Configuration Profiles y creó una configuración de borrador para el clúster. Consulte la documentación de *Administración del ciclo de vida de hosts y clústeres*.

Procedimiento

1 En vSphere Client, desplácese hasta un clúster que administre con una sola imagen.

2 En la pestaña **Configurar**, haga clic en **Estado deseado > Configuración**.

3 En la pestaña **Configuración**, haga clic en **sistema**.

4 Haga clic en **tls_client** o en **tls_server**.

Según si la configuración se modificó anteriormente, haga clic en **Configurar ajustes** o en **Editar**.

5 Seleccione el perfil de TLS en el menú desplegable.

6 Haga clic en **Guardar**.

7 Corrija el clúster según la configuración de borrador.

a Para corregir el clúster según la configuración de borrador, en la pestaña **Borrador**, haga clic en **Aplicar cambios**.

b Siga los pasos del asistente **Corregir**. Para obtener más información, consulte la documentación sobre *Administración del ciclo de vida de hosts y clústeres*.

Resultados

Todos los hosts ESXi del clúster cumplen con la configuración deseada.

Cambiar el perfil de TLS de un host ESXi mediante la CLI

Puede cambiar el perfil de TLS de un host ESXi. El perfil de TLS predeterminado es COMPATIBLE.

Para hosts ESXi independientes y clústeres que no sean de vLCM, debe administrar el perfil de TLS mediante comandos `esxcli`. Para obtener más información, consulte *Referencia de ESXCLI*. Para los hosts ESXi en un clúster de vLCM, puede utilizar vSphere Configuration Profiles o los comandos `esxcli`.

Requisitos previos

Habilite SSH o ESXi Shell en el host ESXi.

Procedimiento

1 Conéctese al host ESXi.

   Puede usar SSH o ESXi Shell.

2 Ponga el host ESXi en modo de mantenimiento.

3 Para cambiar el perfil de TLS, ejecute el siguiente comando.

   ```
   esxcli system tls [client | server] set --profile [COMPATIBLE | NIST_2024 | MANUAL]
   ```

   Nota Si desea realizar cambios en los parámetros de TLS (ya sea en el nivel del sistema o en el nivel de servicio), seleccione el perfil MANUAL.

4 Reinicie el host ESXi para que se apliquen los cambios.

5 Una vez que se reinicie el host ESXi, sáquelo del modo de mantenimiento.

Editar los parámetros del perfil de TLS MANUAL mediante el uso de la CLI

Puede editar el conjunto de parámetros del perfil de TLS MANUAL. Para cambiar los parámetros de TLS, como la lista de cifrado y el paquete de claves de cifrado, primero debe configurar el perfil de TLS en MANUAL.

Advertencia Broadcom no es compatible con el perfil de TLS MANUAL. Solo se admiten los perfiles de TLS COMPATIBLE y NIST_2024. Utilice el perfil de TLS MANUAL bajo su propia responsabilidad.

Debe administrar los parámetros del perfil de TLS MANUAL mediante los comandos `esxcli`. La administración de los parámetros del perfil de TLS MANUAL no está integrada con vSphere Configuration Profiles.

No se pueden establecer parámetros TLS para servicios de vSphere individuales. Los cambios que realice mediante el perfil de TLS MANUAL se aplicarán en el nivel del sistema.

Requisitos previos

Habilite SSH o ESXi Shell en el host ESXi.

Cambie el perfil de TLS a MANUAL. Consulte Cambiar el perfil de TLS de un host ESXi mediante vSphere Client o Cambiar el perfil de TLS de un host ESXi mediante la CLI.

Procedimiento

1 Conéctese al host ESXi.

Puede usar SSH o ESXi Shell.

2 Ponga el host ESXi en modo de mantenimiento.

3 Asegúrese de que el perfil de TLS sea MANUAL.

```
esxcli system tls [client | server] get
```

4 Para cambiar los parámetros, ejecute cualquiera de los siguientes comandos.

```
esxcli system tls [client | server] set --cipher-list=str
esxcli system tls [client | server] set --cipher-suite=str
esxcli system tls [client | server] set --groups=str
esxcli system tls [client | server] set --protocol-versions=str
```

donde *str* es una cadena en estilo OpenSSL que está delimitada por dos puntos, comas o espacios. Por ejemplo: `--cipher-list=ECDHE+AESGCM:ECDHE+AES`

Para obtener más información, ejecute el siguiente comando:

```
esxcli system tls [client | server] set --help
```

5 Reinicie el host ESXi para que se apliquen los cambios.

6 Una vez que se reinicie el host ESXi, sáquelo del modo de mantenimiento.

Ejemplo

En el siguiente ejemplo, primero se establece el perfil de TLS en MANUAL y, a continuación, se establece un conjunto más restrictivo de curvas (grupos). Es necesario reiniciar para que se apliquen los cambios.

```
[root@host1] esxcli system tls server get
   Profile: COMPATIBLE
   Cipher List: <profile default>
   Cipher Suite: <profile default>
   Groups: <profile default>
   Protocol Versions: <profile default>
   Reboot Required: false
[root@host1] esxcli system tls server set --profile MANUAL
[root@host1] esxcli system tls server get
   Profile: MANUAL
   Cipher List: ECDHE+AESGCM:ECDHE+AES
   Cipher Suite: TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384
   Groups: prime256v1:secp384r1:secp521r1
   Protocol Versions: tls1.2,tls1.3
   Reboot Required: true
[root@host1] esxcli system tls server set --groups=prime256v1:secp384r1
[root@host1] esxcli system tls server get
   Profile: MANUAL
   Cipher List: TLS_AES_128_CCM_SHA256
```

```
Cipher Suite: TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384
Groups: prime256v1:secp384r1
Protocol Versions: tls1.2,tls1.3
Reboot Required: true
```

Administrar el perfil de TLS de un host de vCenter Server

Debe utilizar las API para ver y cambiar el perfil de TLS de un host de vCenter Server.

Puede utilizar varias formas de ejecutar solicitudes HTTP. Esta tarea muestra cómo utilizar el Centro para desarrolladores en vSphere Client a fin de administrar perfiles de TLS. Consulte la *Guía de programación de administración de VMware vCenter Server* para obtener más información sobre el uso de las API a fin de administrar vCenter Server Appliance.

Procedimiento

1 Inicie sesión en el sistema vCenter Server mediante vSphere Client.

2 En el menú, seleccione **Centro para desarrolladores**.

3 Haga clic en **API Explorer**.

4 En el menú desplegable **Seleccionar API**, elija **dispositivo**.

   Las siguientes categorías y acciones de API están disponibles.

   Tabla 15-3. API de TLS de vCenter Server

Opción	Categoría de API	Acción asociada
Obtiene la lista de todos los perfiles de TLS y su configuración.	tls/profiles/	GET
Obtiene los parámetros de un perfil de TLS específico.	tls/profiles/{id}	GET
Obtiene el nombre del perfil de TLS actual configurado de manera global.	tls/profiles/global/	GET
Establece uno de los perfiles estándar que se especifica de manera global.	tls/profiles/global/	PUT **Nota** Esta acción reinicia los servicios de vCenter Server.
Obtiene los parámetros del perfil de TLS actual configurado de manera global.	tls/manual-parameters/global	GET

   Nota En este momento, no se pueden modificar los parámetros de un perfil de TLS de vCenter Server.

5 Ejecute el comando deseado.

Privilegios definidos

16

En las siguientes tablas se enumeran los privilegios predeterminados que, cuando se seleccionan para un rol, pueden asignarse a un usuario y a un objeto.

Al establecer permisos, verifique que todos los tipos de objetos estén configurados con los privilegios adecuados para cada acción en particular. Algunas operaciones requieren permiso de acceso en la carpeta raíz o la carpeta primaria además del acceso al objeto que se manipula. Algunas operaciones requieren permiso de acceso o ejecución en la carpeta primaria y un objeto relacionado. Vea también Usar registrador de privilegios.

Las extensiones de vCenter Server pueden definir privilegios adicionales que no están indicados aquí. Consulte la documentación relacionada con las extensiones para obtener más información sobre estos privilegios.

Lea los siguientes temas a continuación:

- Privilegios de extensiones
- Privilegios de proveedor de estadísticas externos
- Privilegios de carpeta
- Privilegios globales
- Los privilegios de interacción con el editor de datos de invitados
- Privilegios del modo vinculado híbrido
- Privilegios de proveedor de actualización de estado
- Privilegios de CIM para hosts
- Privilegios de configuración de hosts
- Privilegios de grupo de entropía de host
- Privilegios de Intel Software Guard Extensions de host
- Privilegios de inventario de host
- Privilegios de operaciones locales en hosts
- Privilegios de estadísticas del host
- Privilegios del módulo de plataforma de confianza del host
- Privilegios de vSphere Replication de host
- Privilegios de perfiles de host
- Privilegios de perfiles de vCenter Server
- Privilegios de espacios de nombres de vSphere
- Privilegios de red
- Privilegios de NSX
- Privilegios de observación de VMware
- Privilegios de OvfManager
- Privilegios de interacción con daemons de REST de socios
- Privilegios de rendimiento
- Privilegios de complemento
- Privilegios de Replicación como servicio
- Privilegios de permisos
- Privilegios de directivas de almacenamiento de máquina virtual
- Privilegios de recursos
- Privilegios para tareas programadas
- Privilegios de sesiones

- Privilegios de vistas de almacenamiento
- Privilegios de servicios de supervisor
- Privilegios de tareas
- Privilegios de administración de tenants
- Privilegios del servicio de transferencia
- Privilegios de VcTrusts/VcIdentity
- Privilegios de administrador de infraestructura de confianza
- Privilegios de vApp
- Privilegios de VcIdentityProviders
- Privilegios de configuración de VMware vSphere Lifecycle Manager
- Privilegios de administración de configuración deseados de VMware vSphere Lifecycle Manager Manager
- Privilegios de perspectiva de estado de ESXi de VMware vSphere Lifecycle Manager
- Privilegios de depósitos de VMware vSphere Lifecycle Manager
- Privilegios generales de VMware vSphere Lifecycle Manager
- Privilegios de compatibilidad de hardware de VMware vSphere Lifecycle Manager
- Privilegios de imagen de VMware vSphere Lifecycle Manager
- Privilegios de corrección de imágenes de VMware vSphere Lifecycle Manager
- Privilegios de configuración de VMware vSphere Lifecycle Manager
- Privilegios de administración de líneas base de VMware vSphere Lifecycle Manager
- Privilegios de administración de revisiones y actualizaciones de VMware vSphere Lifecycle Manager
- Privilegios de carga de archivos de VMware vSphere Lifecycle Manager
- Privilegios de configuración de cambio de máquina virtual
- Privilegios de operaciones de invitado de máquina virtual
- Privilegios para la interacción con máquinas virtuales
- Privilegios de edición de inventario de máquinas virtuales
- Privilegios de aprovisionamiento de las máquinas virtuales
- Privilegios de configuración de servicios de la máquina virtual
- Privilegios de administración de snapshots de las máquinas virtuales
- Privilegios de vSphere Replication de máquinas virtuales
- Privilegios de clases de máquinas virtuales

- Privilegios de vSAN
- Privilegios de estadísticas de vSAN
- Privilegios de zonas de vSphere
- Privilegios de vService
- Privilegios de etiquetado de vSphere
- Privilegios de vSphere Client
- Privilegios de vSphere Data Protection
- Privilegios de estadísticas de vSphere

Privilegios de alarmas

Los privilegios de alarmas controlan la capacidad de crear alarmas, modificarlas y responder a ellas en objetos de inventario.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-1. Privilegios de alarmas

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Confirmar alarma	Permite eliminar todas las acciones de todas las alarmas activadas.	Objeto en el que se define una alarma	Alarm.Acknowledge
Crear alarma	Permite crear una alarma nueva. Al crear alarmas con una acción personalizada, se comprueba el privilegio de realizar la acción cuando el usuario crea la alarma.	Objeto en el que se define una alarma	Alarm.Create
Deshabilitar acción de alarma	Permite evitar que se produzca una acción de alarma después de que se activa la alarma. La alarma en sí no está desactivada.	Objeto en el que se define una alarma	Alarm.DisableActions
Deshabilitar o habilitar la alarma en la entidad	Permite activar o desactivar una alarma en particular en un tipo de destino concreto.	Objeto en el que se puede activar la alarma	Alarm.ToggleEnableOnEntity
Modificar alarma	Permite cambiar las propiedades de una alarma.	Objeto en el que se define una alarma	Alarm.Edit

Tabla 16-1. Privilegios de alarmas (continuación)

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Quitar alarma	Permite eliminar una alarma.	Objeto en el que se define una alarma	Alarm.Delete
Establecer estado de alarma	Permite cambiar el estado de la alarma de evento configurada. El estado puede cambiar a **Normal**, **Advertencia** o **Alerta**.	Objeto en el que se define una alarma	Alarm.SetStatus

Privilegios de Auto Deploy y perfiles de imagen

Los privilegios de Auto Deploy determinan quién puede realizar ciertas tareas en las reglas de Auto Deploy, y quién puede asociar un host. Los privilegios de Auto Deploy también permiten controlar quién puede crear o editar un perfil de imagen.

En la tabla se describen los privilegios que determinan quién puede administrar las reglas y los conjuntos de reglas de Auto Deploy, y quién puede crear y editar perfiles de imagen. Para obtener más información sobre Auto Deploy, consulte la documentación de *Instalar y configurar VMware ESXi*.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-2. Privilegios de Auto Deploy

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
■ **Host** ■ **Equipo asociado**	Permite a los usuarios asociar un host a una máquina.	vCenter Server	AutoDeploy.Host.AssociateMachine
■ **Perfil de imagen** ■ **Crear** ■ **Editar**	**Crear** permite crear perfiles de imagen. **Editar** permite editar perfiles de imagen.	vCenter Server	AutoDeploy.Profile.Create AutoDeploy.Profile.Edit

Tabla 16-2. Privilegios de Auto Deploy (continuación)

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
■ **Regla** ■ **Crear** ■ **Editar** ■ **Eliminar**	**Crear** permite crear reglas de Auto Deploy. **Editar** permite editar reglas de Auto Deploy. **Eliminar** permite eliminar reglas de Auto Deploy.	vCenter Server	AutoDeploy.Rule.Create AutoDeploy.Rule.Edit AutoDeploy.Rule.Delete
■ **Conjunto de reglas** ■ **Activar** ■ **Editar**	**Activar** permite activar conjuntos de reglas de Auto Deploy. **Editar** permite editar conjuntos de reglas de Auto Deploy.	vCenter Server	AutoDeploy.RuleSet.Activate AutoDeploy.RuleSet.Edit

Privilegios de los certificados

Los privilegios de los certificados controlan qué usuarios pueden administrar los certificados de ESXi.

Este privilegio determina quién puede administrar los certificados de los hosts de ESXi. Consulte la sección sobre privilegios necesarios para operaciones de administración de certificados en la documentación de *vSphere Authentication* para obtener información sobre la administración de certificados de vCenter Server.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-3. Privilegios de los certificados de los hosts

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Administrar certificados	Permite administrar los certificados de los hosts de ESXi.	vCenter Server	Certificate.Manage

Privilegios de la entidad de certificación

Los privilegios de la entidad de certificación controlan los aspectos de los certificados de VMware Certificate Authority (VMCA).

Tabla 16-4. Privilegios de la entidad de certificación

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Crear/Eliminar (privilegio de administradores).	Permite el acceso de nivel administrativo completo para administrar certificados vCenter Server.	vCenter Server	CertificateAuthority.Administer
Crear/Eliminar (por debajo del privilegio de administradores).	Permite ver el certificado raíz de VMCA en la página Administración de certificados de vSphere Client.	vCenter Server	CertificateAuthority.Manage

Privilegios de administración de certificados

Los privilegios de administración de certificados controlan qué usuarios pueden administrar los certificados de vCenter Server.

Tabla 16-5. Privilegios de administración de certificados

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Crear/Eliminar (privilegio de administradores).	Permite el acceso de nivel administrativo completo a diversas funcionalidades y API internas para operaciones relacionadas con certificados de vCenter Server.	vCenter Server	CertificateManagement.Administer
Crear/Eliminar (por debajo del privilegio de administradores).	Permite reducir el acceso administrativo a varias API y funcionalidades internas. Este privilegio limita las operaciones relacionadas con certificados para que el usuario no pueda escalar privilegios que no son de administrador. Las operaciones permitidas son las siguientes: ■ Generar solicitudes de firma de certificado ■ Crear y recuperar cadenas raíz de confianza ■ Eliminar cadenas raíz de confianza creadas por un usuario con el privilegio **Administración de certificados.Crear/Eliminar (por debajo del privilegio de administradores).** ■ Recuperar certificados SSL de máquina ■ Recuperar las cadenas de certificados de firma para validar los tokens emitidos por vCenter Server	vCenter Server	CertificateManagement.Manage

Privilegios de CNS

Los privilegios de almacenamiento nativo en la nube (Cloud Native Store, CNS) controlan qué usuarios pueden acceder a la interfaz de usuario de almacenamiento nativo en la nube.

Tabla 16-6. Privilegios de CNS

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Permite búsquedas	Permite al administrador de almacenamiento ver la interfaz de usuario de almacenamiento nativo en la nube.	vCenter Server raíz	Cns.Searchable

Privilegios de directivas de recursos informáticos

Los privilegios de directivas de recursos informáticos controlan la capacidad de administrar políticas de recursos informáticos.

Tabla 16-7. Privilegios de directivas de recursos informáticos

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Crear y eliminar directiva de recursos informáticos	Permite crear y eliminar directivas de recursos informáticos.	vCenter Server raíz	ComputePolicy.Manage

Privilegios de la biblioteca de contenido

Las bibliotecas de contenido ofrecen administración simple y efectiva de plantillas de máquinas virtuales y vApps. Los privilegios de bibliotecas de contenido determinan quién puede ver o administrar diferentes aspectos de las bibliotecas de contenido.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Nota La herencia de permisos para bibliotecas de contenido funciona en el contexto de una única instancia de vCenter Server. No obstante, las bibliotecas de contenido no son elementos secundarios directos de un sistema vCenter Server desde una perspectiva de inventario. El elemento primario directo de las bibliotecas de contenido es la raíz global. Esto significa que, si se configura un permiso a nivel de vCenter Server y se propaga a los objetos secundarios, el permiso se aplica a los centros de datos, las carpetas, los clústeres, los hosts, las máquinas virtuales, etc., pero no a las bibliotecas de contenido que se ven y se manejan con esta instancia de vCenter Server. Para asignar un permiso en una biblioteca de contenido, un administrador debe conceder dicho permiso al usuario como permiso global. Los permisos globales son compatibles con la asignación de privilegios en soluciones de un objeto raíz global.

Tabla 16-8. Privilegios de la biblioteca de contenido

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Agregar elemento de biblioteca	Permite agregar elementos a una biblioteca.	Biblioteca	ContentLibrary.AddLibraryItem
Agregar certificado raíz a almacén de confianza	Permite agregar certificados raíz al almacén de certificados raíz de confianza.	vCenter Server	ContentLibrary.AddCertToTrustStore
Insertar una plantilla	Permite insertar plantillas.	Biblioteca	ContentLibrary.CheckInTemplate
Retirar una plantilla	Permite retirar plantillas.	Biblioteca	ContentLibrary.CheckOutTemplate
Crear una suscripción a una biblioteca publicada	Permite crear una suscripción a una biblioteca.	Biblioteca	ContentLibrary.AddSubscription
Crear biblioteca local	Permite crear bibliotecas locales en el sistema vCenter Server especificado.	vCenter Server	ContentLibrary.CreateLocalLibrary
Crear o eliminar un registro de Harbor	Permite crear o eliminar el servicio de registro de VMware Tanzu Harbor.	vCenter Server para la creación. Registro para la eliminación.	ContentLibrary.ManageRegistry
Crear biblioteca suscrita	Permite crear bibliotecas suscritas.	vCenter Server	ContentLibrary.CreateSubscribedLibrary
Crear, eliminar o purgar un proyecto del registro de Harbor	Permite crear, eliminar o purgar proyectos del registro de VMware Tanzu Harbor.	Registro	ContentLibrary.ManageRegistryProject
Eliminar elemento de biblioteca	Permite eliminar elementos de biblioteca.	Biblioteca. Establezca este permiso para que se propague a todos los elementos de la biblioteca.	ContentLibrary.DeleteLibraryItem
Eliminar biblioteca local	Permite borrar una biblioteca local.	Biblioteca	ContentLibrary.DeleteLocalLibrary

Tabla 16-8. Privilegios de la biblioteca de contenido (continuación)

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Eliminar certificado raíz de almacén de confianza	Permite eliminar certificados raíz del almacén de certificados raíz de confianza.	vCenter Server	ContentLibrary.DeleteCertFromTrustStore
Eliminar biblioteca suscrita	Permite borrar una biblioteca suscrita.	Biblioteca	ContentLibrary.DeleteSubscribedLibrary
Eliminar una suscripción a una biblioteca publicada	Permite eliminar la suscripción a una biblioteca.	Biblioteca	ContentLibrary.DeleteSubscription
Descargar archivos	Permite descargar archivos de la biblioteca de contenido.	Biblioteca	ContentLibrary.DownloadSession
Desalojar elemento de biblioteca	Permite expulsar elementos. El contenido de una biblioteca suscrita puede estar almacenado en caché o no. Si el contenido está almacenado en caché, puede expulsar un elemento de biblioteca para quitarlo (si tiene el privilegio correspondiente).	Biblioteca. Establezca este permiso para que se propague a todos los elementos de la biblioteca.	ContentLibrary.EvictLibraryItem
Desalojar biblioteca suscrita	Permite expulsar una biblioteca suscrita. El contenido de una biblioteca suscrita puede estar almacenado en caché o no. Si el contenido está almacenado en caché, puede expulsar una biblioteca para quitarla (si tiene el privilegio correspondiente).	Biblioteca	ContentLibrary.EvictSubscribedLibrary

Tabla 16-8. Privilegios de la biblioteca de contenido (continuación)

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Importar almacenamiento	Permite a un usuario importar un elemento de biblioteca si la dirección URL del archivo de origen empieza con `ds://` o `file://`. Este privilegio está desactivado para el administrador de bibliotecas de contenido de forma predeterminada. Ya que una importación desde una dirección URL de almacenamiento implica la importación de contenido, active este privilegio solo si es necesario y si no hay riesgos de seguridad con el usuario que realiza la importación.	Biblioteca	ContentLibrary.ImportStorage
Administrar recursos del registro de Harbor en un recurso informático especificado	Permite administrar los recursos del registro de VMware Tanzu Harbor.	Clúster de proceso	ContentLibrary.ManageClusterRegistryResource

Tabla 16-8. Privilegios de la biblioteca de contenido (continuación)

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Sondear información de suscripción	Este privilegio permite a las API y los usuarios de soluciones sondear la información de suscripción de una biblioteca remota, como su dirección URL, certificado SSL y contraseña. La estructura que se obtiene describe si la configuración de suscripción es correcta o si hay problemas, como errores de SSL.	Biblioteca	ContentLibrary.ProbeSubscription
Publicar un elemento de la biblioteca para los suscriptores	Permite publicar elementos de biblioteca para suscriptores.	Biblioteca. Establezca este permiso para que se propague a todos los elementos de la biblioteca.	ContentLibrary.PublishLibraryItem
Publicar una biblioteca para los suscriptores	Permite publicar las bibliotecas para suscriptores.	Biblioteca	ContentLibrary.PublishLibrary
Leer almacenamiento	Permite leer el almacenamiento de una biblioteca de contenido.	Biblioteca	ContentLibrary.ReadStorage
Sincronizar elemento de biblioteca	Permite sincronizar elementos de biblioteca.	Biblioteca. Establezca este permiso para que se propague a todos los elementos de la biblioteca.	ContentLibrary.SyncLibraryItem
Sincronizar biblioteca suscrita	Permite sincronizar bibliotecas suscritas.	Biblioteca	ContentLibrary.SyncLibrary

Tabla 16-8. Privilegios de la biblioteca de contenido (continuación)

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Escribir introspección	Permite a una API o un usuario de solución revisar los complementos de compatibilidad de tipos del servicio de biblioteca de contenido.	Biblioteca	ContentLibrary.TypeIntrospection
Actualizar parámetros de configuración	Permite actualizar los valores de configuración. Ninguno de los elementos de la interfaz de usuario de vSphere Client se asocia con este privilegio.	Biblioteca	ContentLibrary.UpdateConfiguration
Actualizar archivos	Permite cargar contenido a la biblioteca de contenido. También permite eliminar archivos de un elemento de biblioteca.	Biblioteca	ContentLibrary.UpdateSession
Actualizar biblioteca	Permite actualizar la biblioteca de contenido.	Biblioteca	ContentLibrary.UpdateLibrary
Actualizar elemento de biblioteca	Permite actualizar elementos de biblioteca.	Biblioteca. Establezca este permiso para que se propague a todos los elementos de la biblioteca.	ContentLibrary.UpdateLibraryItem
Actualizar biblioteca local	Permite actualizar bibliotecas locales.	Biblioteca	ContentLibrary.UpdateLocalLibrary
Actualizar biblioteca suscrita	Permite actualizar las propiedades de una biblioteca suscrita.	Biblioteca	ContentLibrary.UpdateSubscribedLibrary

Tabla 16-8. Privilegios de la biblioteca de contenido (continuación)

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Actualizar una suscripción a una biblioteca publicada	Permite realizar actualizaciones en los parámetros de suscripción. Los usuarios pueden actualizar parámetros como la especificación de la instancia de vCenter Server de la biblioteca suscrita y la colocación de sus elementos de plantilla de máquina virtual.	Biblioteca	ContentLibrary.UpdateSubscription
Ver parámetros de configuración	Permite ver las opciones de configuración. Ninguno de los elementos de la interfaz de usuario de vSphere Client se asocia con este privilegio.	Biblioteca	ContentLibrary.GetConfiguration

Privilegios de operaciones de cifrado

Los privilegios de operaciones de cifrado controlan quién puede realizar qué tipo de operación criptográfica en qué tipo de objeto.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-9. Privilegios de operaciones criptográficas

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Acceso directo	Permite que los usuarios accedan a los recursos cifrados. Los usuarios pueden exportar máquinas virtuales, tener acceso NFC a las máquinas virtuales y abrir una sesión de consola en una máquina virtual cifrada.	Máquina virtual, host o almacén de datos	Cryptographer.Access
Agregar disco	Permite que los usuarios agreguen un disco a una máquina virtual cifrada.	Máquina virtual	Cryptographer.AddDisk
Clonar	Permite que los usuarios clonen una máquina virtual cifrada.	Máquina virtual	Cryptographer.Clone
Descifrar	Permite que los usuarios descifren una máquina virtual o un disco.	Máquina virtual	Cryptographer.Decrypt
Cifrar	Permite que los usuarios cifren una máquina virtual o un disco de máquina virtual.	Máquina virtual	Cryptographer.Encrypt

Tabla 16-9. Privilegios de operaciones criptográficas (continuación)

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Cifrar nuevo	Permite que los usuarios cifren una máquina virtual durante la creación de una máquina virtual o un disco durante la creación de un disco.	Carpeta de máquina virtual	Cryptographer.EncryptNew
Administrar directivas de cifrado	Permite que los usuarios administren las directivas de almacenamiento de la máquina virtual con filtros de E/S de cifrado. De forma predeterminada, las máquinas virtuales que utilizan la directiva de almacenamiento Cifrado no utilizan otras directivas de almacenamiento.	Carpeta raíz de vCenter Server	Cryptographer.ManageEncryptionPolicy

Tabla 16-9. Privilegios de operaciones criptográficas (continuación)

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Administrar KMS	Permite que los usuarios administren el servidor de administración de claves (Key Management Server, KMS) para el sistema vCenter Server. Entre las tareas de administración, se incluyen agregar y eliminar instancias de KMS y establecer una relación de confianza con el KMS.	Sistema vCenter Server	Cryptographer.ManageKeyServers
Administrar claves	Permite que los usuarios realicen operaciones de administración de claves. Estas operaciones no se admiten en vSphere Client, pero se pueden realizar mediante el uso de `crypto-util` o la API.	Carpeta raíz de vCenter Server	Cryptographer.ManageKeys

Tabla 16-9. Privilegios de operaciones criptográficas (continuación)

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Migrar	Permite que los usuarios migren una máquina virtual cifrada a un host ESXi distinto. Admite la migración con o sin vMotion y Storage vMotion. Admite la migración a una instancia de vCenter Server distinta.	Máquina virtual	Cryptographer.Migrate
Volver a cifrar	Permite que los usuarios vuelvan a cifrar máquinas virtuales o discos con una clave distinta. Este privilegio es necesario para las operaciones de repetición de cifrado profundo y superficial.	Máquina virtual	Cryptographer.Recrypt
Registrar máquina virtual	Permite que los usuarios registren una máquina virtual cifrada con un host ESXi.	Carpeta de máquina virtual	Cryptographer.RegisterVM

Tabla 16-9. Privilegios de operaciones criptográficas (continuación)

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Registrar host	Permite que los usuarios habiliten el cifrado en un host. El cifrado en un host se puede habilitar de forma explícita o mediante el proceso de creación de máquinas virtuales.	Carpeta de hosts para los hosts independientes, clúster para los hosts del clúster	Cryptographer.RegisterHost
Leer información de KMS	Permite a los usuarios enumerar proveedores de claves nativos de vSphere en el vCenter Server y en los hosts. También permite a los usuarios obtener información del proveedor de claves nativo de vSphere.	vCenter Server o host	Cryptographer.ReadKeyServersInfo

Privilegios de grupo dvPort

Los privilegios de grupo de puertos virtuales distribuidos controlan la capacidad para crear, eliminar y modificar grupos de puertos virtuales distribuidos.

En la tabla se describen los privilegios necesarios para crear y configurar grupos de puertos virtuales distribuidos.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-10. Privilegios del grupo de puertos virtuales distribuidos

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Crear	Permite crear un grupo de puertos virtuales distribuidos.	Grupos de puertos virtuales	DVPortgroup.Create
Eliminar	Permite eliminar un grupo de puertos virtuales distribuidos. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	Grupos de puertos virtuales	DVPortgroup.Delete
Modificar	Permite modificar la configuración de un grupo de puertos virtuales distribuidos.	Grupos de puertos virtuales	DVPortgroup.Modify
Operación de directiva	Permite configurar la directiva de un grupo de puertos virtuales distribuidos.	Grupos de puertos virtuales	DVPortgroup.PolicyOp
Operación de ámbito	Permite configurar el ámbito de un grupo de puertos virtuales distribuidos.	Grupos de puertos virtuales	DVPortgroup.ScopeOp

Privilegios de Distributed Switch

Los privilegios de Distributed Switch controlan la capacidad para realizar tareas relacionadas con la administración de las instancias de Distributed Switch.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-11. Privilegios de vSphere Distributed Switch

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Crear	Permite crear un conmutador distribuido.	Centros de datos, carpetas de red	DVSwitch.Create
Eliminar	Permite quitar un conmutador distribuido. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	Conmutadores distribuidos	DVSwitch.Delete
Operación de host	Permite cambiar los miembros de host de un conmutador distribuido.	Conmutadores distribuidos	DVSwitch.HostOp
Modificar	Permite cambiar la configuración de un conmutador distribuido.	Conmutadores distribuidos	DVSwitch.Modify
Mover	Permite mover vSphere Distributed Switch a otra carpeta.	Conmutadores distribuidos	DVSwitch.Move
Operación Network I/O Control	Permite cambiar la configuración de los recursos de vSphere Distributed Switch.	Conmutadores distribuidos	DVSwitch.ResourceManagement
Operación de directiva	Permite cambiar la directiva de vSphere Distributed Switch.	Conmutadores distribuidos	DVSwitch.PolicyOp
Operación de configuración de puerto	Permite cambiar los parámetros de un puerto en vSphere Distributed Switch.	Conmutadores distribuidos	DVSwitch.PortConfig
Operación de configuración de puerto	Permite cambiar la configuración de un puerto en vSphere Distributed Switch.	Conmutadores distribuidos	DVSwitch.PortSetting
Operación de VSPAN	Permite cambiar la configuración de VSPAN de vSphere Distributed Switch.	Conmutadores distribuidos	DVSwitch.Vspan

Privilegios de centro de datos

Los privilegios de centro de datos controlan la habilidad para crear y editar centros de datos en el inventario vSphere Client.

Todos los privilegios de centros de datos se utilizan solamente en vCenter Server. El privilegio **Crear centro de datos** se define en carpetas del centro de datos o el objeto raíz. Todos los demás privilegios de centros de datos se emparejan con centros de datos, carpetas de centros de datos o el objeto raíz.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-12. Privilegios de centro de datos

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Crear centro de datos	Permite la creación de un nuevo centro de datos.	Carpeta de centro de datos u objeto raíz	Datacenter.Create
Mover centro de datos	Permite mover un centro de datos. El privilegio debe estar presente tanto en el origen como en el destino.	Centro de datos, origen y destino	Datacenter.Move
Configuración de perfil de protocolo de red	Permite la configuración del perfil de red para un centro de datos.	Centro de datos	Datacenter.IpPoolConfig
Consultar asignación de grupo de direcciones IP	Permite la configuración de un grupo de direcciones IP.	Centro de datos	Datacenter.IpPoolQueryAllocations
Volver a configurar centro de datos	Permite la reconfiguración de un centro de datos.	Centro de datos	Datacenter.Reconfigure
Liberar asignación de IP	Permite liberar la asignación de IP asignada para un centro de datos.	Centro de datos	Datacenter.IpPoolReleaseIp
Quitar centro de datos	Permite la eliminación de un centro de datos. Para tener los permisos necesarios para realizar esta operación, debe tener este privilegio asignado tanto en el objeto como en su objeto principal.	Centro de datos más objeto primario	Datacenter.Delete
Cambiar nombre de centro de datos	Permite cambiarle el nombre a un centro de datos.	Centro de datos	Datacenter.Rename
Actualizar información de Carbon del centro de datos	Permite recopilar métricas relacionadas con la medición de la energía y del carbono.	Centro de datos	Datacenter.UpdateCarbonInfo

Privilegios de almacenes de datos

Los privilegios de almacenes de datos controlan la capacidad para examinar y administrar almacenes de datos, así como para asignar espacios en ellos.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-13. Privilegios de almacenes de datos

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Asignar espacio	Permite asignar un espacio en un almacén de datos de una máquina virtual, una instantánea, un clon o un disco virtual.	Almacenes de datos	Datastore.AllocateSpace
Examinar almacén de datos	Permite desplazarse hasta archivos de un almacén de datos.	Almacenes de datos	Datastore.Browse
Configurar la administración de E/S del almacén de datos	Permite configurar Storage I/O Control.	Almacenes de datos	Datastore.ConfigIOManagement
Configurar almacén de datos	Permite configurar un almacén de datos.	Almacenes de datos	Datastore.Config
Operaciones de archivos de bajo nivel	Permite realizar tareas de lectura, escritura, eliminación y cambio de nombre en el explorador del almacén de datos.	Almacenes de datos	Datastore.FileManagement

Tabla 16-13. Privilegios de almacenes de datos (continuación)

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Mover almacén de datos	Permite mover un almacén de datos entre diferentes carpetas. Los privilegios deben estar presentes tanto en el origen como en el destino.	Almacén de datos, origen y destino	Datastore.Move
Quitar almacén de datos	Permite quitar un almacén de datos. Este privilegio es obsoleto. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	Almacenes de datos	Datastore.Delete
Quitar archivo	Permite eliminar archivos del almacén de datos. Este privilegio es obsoleto. Asigne el privilegio **Operaciones de archivos de nivel bajo**.	Almacenes de datos	Datastore.DeleteFile
Cambiar nombre de almacén de datos	Permite cambiar el nombre de un almacén de datos.	Almacenes de datos	Datastore.Rename

Tabla 16-13. Privilegios de almacenes de datos (continuación)

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Actualizar archivos de la máquina virtual	Permite actualizar las rutas de acceso de los archivos de máquinas virtuales en un almacén de datos una vez que el almacén de datos se volvió a firmar.	Almacenes de datos	Datastore.UpdateVirtualMachineFiles
Actualizar metadatos de la máquina virtual	Permite actualizar los metadatos de máquina virtual asociados con un almacén de datos.	Almacenes de datos	Datastore.UpdateVirtualMachineMetadata

Privilegios de clústeres de almacenes de datos

Los privilegios de clústeres de almacenes de datos controlan la configuración de clústeres de almacenes de datos de Storage DRS.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-14. Privilegios de clústeres de almacenes de datos

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Configurar un clúster de almacenes de datos	Permite crear y configurar parámetros para los clústeres de almacenes de datos de Storage DRS.	Clústeres de almacenes de datos	StoragePod.Config

Privilegios de ESX Agent Manager

Los privilegios de ESX Agent Manager controlan las operaciones relacionadas con ESX Agent Manager y las máquinas virtuales de agentes. ESX Agent Manager es un servicio que permite instalar máquinas virtuales de administración asociadas a un host que no se ven afectadas por VMware DRS u otros servicios de migración de máquinas virtuales.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-15. ESX Agent Manager

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Configurar	Permite implementar la máquina virtual de un agente en un host o un clúster.	Máquinas virtuales	EAM.Config
Modificar	Permite modificar la máquina virtual de un agente, por ejemplo, apagar o eliminar la máquina virtual.	Máquinas virtuales	EAM.Modify
Ver	Permite ver la máquina virtual de un agente.	Máquinas virtuales	EAM.View

Privilegios de extensiones

Los privilegios de extensiones controlan la capacidad para instalar y administrar extensiones.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-16. Privilegios de extensiones

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Registrar extensión	Permite registrar una extensión (complemento).	vCenter Server raíz	Extension.Register
Eliminar extensión del registro	Permite anular el registro de una extensión (complemento).	vCenter Server raíz	Extension.Unregister
Actualizar extensión	Permite actualizar una extensión (complemento).	vCenter Server raíz	Extension.Update

Privilegios de proveedor de estadísticas externos

Los privilegios del proveedor de estadísticas externo controlan la capacidad para notificar a vCenter Server sobre las estadísticas de Distributed Resource Scheduler (DRS) proactivo.

Estos privilegios solo se aplican a las API internas de VMware.

Privilegios de carpeta

Estos privilegios controlan la capacidad para crear y administrar carpetas.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-17. Privilegios de carpeta

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Crear carpeta	Permite crear una carpeta nueva.	Carpetas	Folder.Create
Eliminar carpeta	Permite eliminar una carpeta. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	Carpetas	Folder.Delete
Mover carpeta	Permite mover una carpeta. El privilegio debe estar presente tanto en el origen como en el destino.	Carpetas	Folder.Move
Cambiar nombre de carpeta	Permite cambiarle el nombre a una carpeta.	Carpetas	Folder.Rename

Privilegios globales

Los privilegios globales controlan tareas globales relacionadas con tareas, scripts y extensiones.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-18. Privilegios globales

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Actuar como vCenter Server	Permite preparar e iniciar una operación de envío o recepción de vMotion.	vCenter Server raíz	Global.VCServer
Cancelar tarea	Permite cancelar una tarea en cola o en ejecución.	Objeto de inventario relacionado con la tarea	Global.CancelTask
Planificación de capacidad	Permite activar el uso de la planificación de capacidad para la consolidación de planificación de máquinas físicas en máquinas virtuales.	vCenter Server raíz	Global.CapacityPlanning
Diagnósticos	Permite recuperar una lista de archivos de diagnóstico, encabezados de registro, archivos binarios o paquetes de diagnóstico. Para evitar infracciones de seguridad potenciales, limite este privilegio a la función de administrador de vCenter Server.	vCenter Server raíz	Global.Diagnostics
Deshabilitar métodos	Permite a los servidores de las extensiones de vCenter Server desactivar ciertas operaciones en objetos administrados con vCenter Server.	vCenter Server raíz	Global.DisableMethods
Habilitar métodos	Permite a los servidores de las extensiones de vCenter Server activar ciertas operaciones en objetos administrados con vCenter Server.	vCenter Server raíz	Global.EnableMethods
Etiqueta global	Permite agregar o quitar etiquetas globales.	Host raíz o vCenter Server	Global.GlobalTag
Estado	Permite ver el estado de los componentes de vCenter Server.	vCenter Server raíz	Global.Health
Licencias	Permite ver las licencias instaladas y agregar o quitar licencias.	Host raíz o vCenter Server	Global.Licenses
Registrar evento	Permite registrar un evento definido por el usuario ante una entidad administrada en particular.	Cualquier objeto	Global.LogEvent
Administrar atributos personalizados	Permite agregar y quitar definiciones de campo personalizadas, así como cambiar sus nombres.	vCenter Server raíz	Global.ManageCustomFields

Tabla 16-18. Privilegios globales (continuación)

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Proxy	Permite acceder a una interfaz interna para agregar o quitar puntos extremos en el proxy o desde él.	vCenter Server raíz	Global.Proxy
Acción de script	Permite programar una acción generada por script junto con una alarma.	Cualquier objeto	Global.ScriptAction
Administradores de servicios	Permite utilizar el comando `resxtop` en ESXCLI.	Host raíz o vCenter Server	Global.ServiceManagers
Configurar atributo personalizado	Permite ver, crear o quitar atributos personalizados para un objeto administrado.	Cualquier objeto	Global.SetCustomField
Configuración	Permite leer y modificar las opciones de configuración de vCenter Server de tiempo de ejecución.	vCenter Server raíz	Global.Settings
Etiqueta del sistema	Permite agregar o quitar etiquetas de sistema.	vCenter Server raíz	Global.SystemTag

Los privilegios de interacción con el editor de datos de invitados

Los privilegios de interacción con el editor de datos de invitados controlan el acceso a los datos de invitados publicados en el servicio GDP del host.

Tabla 16-19. Los privilegios de interacción con el editor de datos de invitados

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Suscribirse al servicio de editor de datos del invitado en hosts ESX	Permite acceder a los datos de invitados publicados en el servicio GDP del host.	Hosts	GuestDataPublisher.GetData

Privilegios del modo vinculado híbrido

Los privilegios del modo vinculado híbrido controlan los aspectos de la vinculación de la instancia de vCenter Server en la nube con un dominio vCenter Single Sign-On local. (Se aplica a VMware Cloud on AWS).

Tabla 16-20. Privilegios del modo vinculado híbrido

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Crear	Permite el acceso de nivel administrativo completo para crear y eliminar comunidades.	SDDC	HLM.Create
Administrar	Permite crear confianza para los orígenes y acceder a comunidades (nivel de lectura).	SDDC	HLM.Manage

Privilegios de proveedor de actualización de estado

Los privilegios del proveedor de actualizaciones de estado controlan la capacidad de los proveedores de hardware para notificar a vCenter Server sobre los eventos proactivos de HA.

Estos privilegios solo se aplican a las API internas de VMware.

Privilegios de CIM para hosts

Los privilegios de CIM para hosts controlan el uso de CIM para supervisar el estado de los hosts.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-21. Privilegios de CIM para hosts

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
■ **CIM** ■ **Interacción de CIM**	Permite que un cliente obtenga un ticket para usar los servicios de CIM.	Hosts	Host.Cim.CimInteraction

Privilegios de configuración de hosts

Los privilegios de configuración de hosts controlan la capacidad para configurar hosts.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-22. Privilegios de configuración de hosts

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Configuración **Configuración avanzada**	Permite establecer las opciones de configuración avanzada del host.	Hosts	Host.Config.AdvancedConfig
Configuración **Almacén de autenticación**	Permite configurar los almacenes de autenticación de Active Directory.	Hosts	Host.Config.AuthenticationStore
Configuración **Cambiar configuración de PciPassthru**	Permite cambiar la configuración de PciPassthru de un host.	Hosts	Host.Config.PciPassthru
Configuración **Cambiar configuración de SNMP**	Permite cambiar la configuración de SNMP de un host.	Hosts	Host.Config.Snmp
Configuración **Cambiar configuración de fecha y hora**	Permite cambiar la configuración de fecha y hora de un host.	Hosts	Host.Config.DateTime
Configuración **Cambiar configuración**	Permite configurar el modo de bloqueo de los hosts ESXi.	Hosts	Host.Config.Settings
Configuración **Conexión**	Permite cambiar el estado de conexión de un host (conectado o desconectado).	Hosts	Host.Config.Connection
Configuración **Firmware**	Permite actualizar el firmware del host ESXi.	Hosts	Host.Config.Firmware
Configuración **Configuración de GuestStore**	Permite realizar cambios en GuestStore.	Repositorio de GuestStore	Host.Config.GuestStore
Configuración **Hiperproceso**	Permite activar y desactivar la función de hiperproceso en el programador de la CPU del host.	Hosts	Host.Config.HyperThreading
Configuración **Configuración de imagen**	Permite cambiar la imagen asociada a un host.		Host.Config.Image
Configuración **Mantenimiento**	Permite que el host entre y salga del modo de mantenimiento, y apagar y reiniciar el host.	Hosts	Host.Config.Maintenance

Tabla 16-22. Privilegios de configuración de hosts (continuación)

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
■ **Configuración** ■ **Configuración de memoria**	Permite modificar la configuración del host.	Hosts	Host.Config.Memory
■ **Configuración** ■ **NVDIMM**	Permite leer y configurar DIMM no volátiles.	Hosts	Host.Config.Nvdimm
■ **Configuración** ■ **Configuración de red**	Permite configurar la red, el firewall y la red vMotion.	Hosts	Host.Config.Network
■ **Configuración** ■ **Alimentación**	Permite configurar las opciones de administración de energía del host.	Hosts	Host.Config.Power
■ **Configuración** ■ **Configuración de ProductLocker**	Permite configurar la carpeta productlocker de ESXi.	Hosts	Host.Config.ProductLocker
■ **Configuración** ■ **Cuarentena**	Permite poner un host en modo de cuarentena.	Hosts	Host.Config.Quarantine
■ **Configuración** ■ **Consultar revisión**	Permite consultar las revisiones instalables e instalar revisiones en el host.	Hosts	Host.Config.Patch
■ **Configuración** ■ **Perfil de seguridad y firewall**	Permite configurar los servicios de Internet, como SSH, Telnet, SNMP y del firewall del host.	Hosts	Host.Config.NetService
■ **Configuración** ■ **Configuración de partición de almacenamiento**	Permite administrar la partición de diagnóstico y el almacén de datos de VMFS. Los usuarios con este privilegio pueden examinar dispositivos de almacenamiento nuevos y administrar iSCSI.	Hosts	Host.Config.Storage
■ **Configuración** ■ **Administración del sistema**	Permite que las extensiones manipulen el sistema de archivos del host.	Hosts	Host.Config.SystemManagement

Tabla 16-22. Privilegios de configuración de hosts (continuación)

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
■ **Configuración** ■ **Recursos del sistema**	Permite actualizar la configuración de la jerarquía de recursos del sistema.	Hosts	Host.Config.Resources
■ **Configuración** ■ **Configuración de inicio automático de la máquina virtual**	Permite cambiar el orden de inicio e interrupción automáticos de las máquinas virtuales de un solo host.	Hosts	Host.Config.AutoStart

Privilegios de grupo de entropía de host

Los privilegios de grupo de entropía de host controlan la capacidad de ver y agregar la entropía de ESXi.

Tabla 16-23. Privilegios de grupo de entropía de host

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
■ **Grupo de entropía** ■ **Leer**	Permite leer la información del grupo de entropía del host.	Hosts	Host.Entropy.Read
■ **Grupo de entropía** ■ **Escribir**	Permite agregar entropía al grupo de entropía de host.	Hosts	Host.Entropy.Write

Privilegios de Intel Software Guard Extensions de host

Los privilegios de Intel Software Guard Extensions de host controlan aspectos de la atestación remota en hosts ESXi de varios sockets.

Tabla 16-24. Privilegios de Intel Software Guard Extensions (SGX) de host

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
■ **Intel Software Guard Extensions (SGX)** ■ **Host de registro de Intel Software Guard Extensions (SGX)**	Permite registrar hosts con el servicio de registro de Intel SGX (para que las cargas de trabajo de SGX puedan realizar la atestación remota de SGX cuando se ejecutan en hosts compatibles con SGX de varios sockets).	Hosts	Host.Sgx.Register

Privilegios de inventario de host

Los privilegios de inventario de host controlan las operaciones de agregar hosts al inventario y a los clústeres, y de mover los hosts en el inventario.

En la tabla se describen los privilegios necesarios para agregar y mover hosts y clústeres en el inventario.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-25. Privilegios de inventario de host

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
■ **Inventario** ■ **Agregar host a clúster**	Permite agregar un host a un clúster que ya existe.	Clústeres	Host.Inventory.AddHostToCluster
■ **Inventario** ■ **Agregar host independiente**	Permite agregar un host independiente.	Carpetas de hosts	Host.Inventory.AddStandaloneHost
■ **Inventario** ■ **Crear clúster**	Permite crear un nuevo clúster.	Carpetas de hosts	Host.Inventory.CreateCluster
■ **Inventario** ■ **Administrar el ciclo de vida del clúster**	Permite administrar el clúster.	Clústeres	Host.Inventory.ManageClusterLifecyle
■ **Inventario** ■ **Modificar clúster**	Permite cambiar las propiedades de un clúster.	Clústeres	Host.Inventory.EditCluster
■ **Inventario** ■ **Mover clúster o host independiente**	Permite mover un clúster o un host independiente entre carpetas. El privilegio debe estar presente tanto en el origen como en el destino.	Clústeres	Host.Inventory.MoveCluster
■ **Inventario** ■ **Mover host**	Permite mover un conjunto de hosts existentes hacia adentro o afuera de un clúster. El privilegio debe estar presente tanto en el origen como en el destino.	Clústeres	Host.Inventory.MoveHost

Tabla 16-25. Privilegios de inventario de host (continuación)

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
■ **Inventario** ■ **Quitar clúster**	Permite eliminar un clúster o un host independiente. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	Clústeres, hosts	Host.Inventory.DeleteCluster
■ **Inventario** ■ **Quitar host**	Permite quitar un host. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	Hosts más objeto primario	Host.Inventory.RemoveHostFromCluster
■ **Inventario** ■ **Cambiar nombre de clúster**	Permite cambiar el nombre de un clúster.	Clústeres	Host.Inventory.RenameCluster

Privilegios de operaciones locales en hosts

Los privilegios de operaciones locales en hosts controlan las acciones que se realizan cuando VMware Host Client está conectado directamente a un host.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-26. Privilegios de operaciones locales en hosts

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
■ **Operaciones locales** ■ **Agregar host a vCenter**	Permite instalar y quitar agentes de vCenter, como vpxa y aam, en un host.	Host raíz	Host.Local.InstallAgent
■ **Operaciones locales** ■ **Crear máquina virtual**	Permite crear una máquina virtual nueva desde cero en un disco sin registrarla en el host.	Host raíz	Host.Local.CreateVM

Tabla 16-26. Privilegios de operaciones locales en hosts (continuación)

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
■ **Operaciones locales** ■ **Eliminar máquina virtual**	Permite eliminar una máquina virtual del disco. Esta operación se admite para máquinas virtuales registradas o no registradas.	Host raíz	Host.Local.DeleteVM
■ **Operaciones locales** ■ **Administrar grupos de usuarios**	Permite administrar cuentas locales en un host.	Host raíz	Host.Local.ManageUserGroups
■ **Operaciones locales** ■ **Volver a configurar máquina virtual**	Permite volver a configurar una máquina virtual.	Host raíz	Host.Local.ReconfigVM

Privilegios de estadísticas del host

Los privilegios de estadísticas de host controlan la capacidad de acceder a la información estadística desde una unidad de procesamiento de datos (Data Processing Unit, DPU).

Estos privilegios solo se aplican a las API internas de VMware.

Privilegios del módulo de plataforma de confianza del host

Los privilegios del módulo de plataforma de confianza del host controlan las operaciones relacionadas con la administración de los chips del módulo de plataforma de confianza (Trusted Platform Module, TPM).

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-27. Privilegios del módulo de plataforma de confianza del host

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
■ **Módulo de plataforma de confianza** ■ **Lectura** ■ **Eliminación de sello**	**Lectura** permite leer información detallada sobre el estado del TPM instalado en el host ESXi. **Eliminación de sello** permite solicitar un host ESXi para descifrar un desafío que pruebe su estado.	Hosts	Host.Tpm.Read Host.Tpm.Unseal

Privilegios de vSphere Replication de host

Los privilegios de vSphere Replication de host controlan la utilización de la replicación de máquinas virtuales que realiza VMware vCenter Site Recovery Manager™ para un host.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-28. Privilegios de vSphere Replication de host

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
■ **vSphere Replication** ■ **Administrar replicación**	Permite administrar la replicación de máquinas virtuales en este host.	Hosts	Host.Hbr.HbrManagement

Privilegios de perfiles de host

Los privilegios de perfiles de host controlan las operaciones relacionadas con la creación y la modificación de perfiles de host.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-29. Privilegios de perfiles de host

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Borrar	Permite borrar información relacionada con el perfil.	vCenter Server raíz	Profile.Clear
Crear	Permite crear un perfil de host.	vCenter Server raíz	Profile.Create
Eliminar	Permite eliminar un perfil de host.	vCenter Server raíz	Profile.Delete
Editar	Permite editar un perfil de host.	vCenter Server raíz	Profile.Edit
Exportar	Permite exportar un perfil de host.	vCenter Server raíz	Profile.Export
Ver	Permite ver un perfil de host.	vCenter Server raíz	Profile.View

Privilegios de perfiles de vCenter Server

Los privilegios de perfiles de vCenter Server controlan aspectos de la enumeración de perfiles, y la exportación e importación de configuraciones desde una instancia de vCenter Server a otra.

Tabla 16-30. Privilegios de perfiles de vCenter Server

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Privilegios de lectura de perfiles de vCenter Server	Permite enumerar y exportar perfiles de vCenter Server.	vCenter Server	Infraprofile.Read
Privilegios de escritura de perfiles de vCenter Server	Permite importar un perfil en otra instancia de vCenter Server y validarlo.	vCenter Server	Infraprofile.Write

Privilegios de espacios de nombres de vSphere

Los privilegios de espacios de nombres controlan quién puede crear y administrar espacios de nombres de VMware vSphere® with VMware Tanzu™.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-31. Privilegios de espacios de nombres

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Permite operaciones de retiro de disco	Permite realizar operaciones de retirada de almacenes de datos.	Almacenes de datos	Namespaces.ManageDisks
Archivos de componentes de cargas de trabajo de copia de seguridad	Permite realizar una copia de seguridad del contenido del clúster etcd (solo se utiliza en VMware Cloud on AWS).	Clústeres	Namespaces.Backup
Espacios de nombres accesibles en lista	Permite enumerar los espacios de nombres accesibles.	Clústeres	Namespaces.ListAccess
Modificar configuración de todo el clúster	Permite modificar la configuración de todo el clúster y activar y desactivar los espacios de nombres del clúster.	Clústeres	Namespaces.Manage

Tabla 16-31. Privilegios de espacios de nombres (continuación)

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Modificar configuración de autoservicio del espacio de nombres en todo el clúster	Permite modificar la configuración de autoservicio del espacio de nombres.	Clústeres (para activar y desactivar) Plantillas (para modificar la configuración) vCenter Server (para crear una plantilla)	Namespaces.SelfServiceManage
Modificar configuración del espacio de nombres	Permite modificar las opciones de configuración de los espacios de nombres, como la asignación de recursos y los permisos de usuario.	Clústeres	Namespaces.Configure
Alternar capacidades de clúster	Permite manipular el estado de las capacidades del clúster (se utiliza internamente solo para VMware Cloud on AWS).	Clústeres	Namespaces.ManageCapabilities
Actualizar clústeres a versiones más recientes	Permite el inicio de la actualización del clúster.	Clústeres	Namespaces.Upgrade

Privilegios de red

Los privilegios de red controlan las tareas relacionadas con la administración de redes.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-32. Privilegios de red

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Asignar red	Permite asignar una red a una máquina virtual.	Redes, máquinas virtuales	Network.Assign
Configurar	Permite configurar una red.	Redes, máquinas virtuales	Network.Config

Tabla 16-32. Privilegios de red (continuación)

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Mover red	Permite mover una red entre carpetas. El privilegio debe estar presente tanto en el origen como en el destino.	Redes	Network.Move
Quitar	Permite eliminar una red. Este privilegio es obsoleto. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	Redes	Network.Delete

Privilegios de NSX

Los privilegios de NSX controlan las tareas relacionadas con la administración de NSX.

Tabla 16-33. Privilegios de NSX

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Leer la configuración de NSX	Permite leer objetos NSX.	NSX	Nsx.Read
Administrar la configuración de NSX	Permite administrar objetos NSX desde la perspectiva del administrador de vSphere.	NSX	Nsx.Manage
Modificar la configuración de NSX	Permite administrar objetos NSX desde la perspectiva del administrador de empresa.	NSX	Nsx.ModifyAll

Privilegios de observación de VMware

Los privilegios de observación de VMware controlan la capacidad de un agente para acceder a las API de observación en vCenter Server.

Estos privilegios solo se aplican a las API internas de VMware.

Privilegios de OvfManager

Los privilegios de OvfManager controlan la capacidad de acceder a vService Manager.

Estos privilegios solo se aplican a las API internas de VMware.

Privilegios de interacción con daemons de REST de socios

Los privilegios de interacción con daemons de REST de socios controlan el acceso a las operaciones de lectura y escritura.

Tabla 16-34. Privilegios de interacción con daemons de REST de socios

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Realizar una operación GET desde el daemon de REST de un socio	Permite al cliente REST aprovisionado por el socio realizar operaciones GET.	El usuario del socio que realiza operaciones GET.	PartnerRestDaemon.Read
Realizar una operación de modificación en el daemon de REST de un socio	Permite al cliente REST aprovisionado por el socio realizar operaciones POST, PUT y DELETE.	El usuario del socio que realiza operaciones POST, PUT o DELETE.	PartnerRestDaemon.Write

Privilegios de rendimiento

Los privilegios de rendimiento controlan la modificación de la configuración de estadísticas de rendimiento.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-35. Privilegios de rendimiento

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Modificar intervalos	Permite crear, quitar y actualizar intervalos de recopilación de datos de rendimiento.	vCenter Server raíz	Performance.ModifyIntervals

Privilegios de complemento

Los privilegios de complemento controlan la administración de los complementos de vSphere Client.

Tabla 16-36. Privilegios de complemento

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Administrar complementos	Permite administrar complementos de vSphere Client.	vCenter Server	Plugin.Management

Privilegios de Replicación como servicio

Los privilegios de replicación como servicio controlan el acceso a varias API internas y funcionalidades relacionadas con la vinculación de vCenter Server.

Estos privilegios solo se aplican a las API internas de VMware.

Privilegios de permisos

Los privilegios de permisos controlan la asignación de funciones y permisos.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-37. Privilegios de permisos

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Modificar permiso	Permite definir una o más reglas de permiso en una entidad, o actualizar reglas si estas ya están presentes para un usuario o grupo determinados en la entidad. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	Cualquier objeto más objeto primario	Authorization.ModifyPermissions
Modificar privilegio	Permite modificar un grupo o una descripción del privilegio. Ninguno de los elementos de la interfaz de usuario de vSphere Client se asocia con este privilegio.	Cualquier objeto	Authorization.ModifyPrivileges
Modificar función	Permite actualizar el nombre de una función y los privilegios asociados con esa función.	Cualquier objeto	Authorization.ModifyRoles
Modificar vTContainer	Permite crear, actualizar y eliminar instancias de vTContainer.	Objetos de vTContainer	Authorization.ModifyVTContainers
Modificar asignaciones de vTContainer	Permite crear y eliminar una asignación de vTContainer.	Objetos de asignación de vTContainer	Authorization.ModifyVTContainerMappings
Reasignar permisos de función	Permite reasignar todos los permisos de una función a otra.	Cualquier objeto	Authorization.ReassignRolePermissions

Privilegios de directivas de almacenamiento de máquina virtual

Los privilegios de almacenamiento de máquina virtual controlan las operaciones relacionadas con los perfiles de almacenamiento.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-38. Privilegios de almacenamiento de la máquina virtual

Nombre del privilegio	Descripción	Necesario para	Nombre de privilegio en la API
Actualizar las directivas de almacenamiento de máquina virtual	Permite realizar cambios en los perfiles de almacenamiento, por ejemplo, crear y actualizar capacidades de almacenamiento y perfiles de almacenamiento de máquinas virtuales.	vCenter Server raíz	StorageProfile. Update
Ver las directivas de almacenamiento de máquina virtual	Permite ver las capacidades de almacenamiento y los perfiles de almacenamiento definidos.	vCenter Server raíz	Perfil de almacenamient o.Ver

Privilegios de recursos

Los privilegios de recursos controlan la creación y la administración de grupos de recursos, como también la migración de máquinas virtuales.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-39. Privilegios de recursos

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Aplicar recomendación	Permite aceptar una sugerencia del servidor para realizar una migración con vMotion.	Clústeres	Resource.ApplyRecommendation
Asignar vApp a grupo de recursos	Permite asignar una vApp a un grupo de recursos.	Grupos de recursos	Resource.AssignVAppToPool
Asignar máquina virtual a grupo de recursos	Permite asignar una máquina virtual a un grupo de recursos.	Grupos de recursos	Resource.AssignVMToPool
Crear grupo de recursos	Permite crear grupos de recursos.	Grupos de recursos, clústeres	Resource.CreatePool
Migrar máquina virtual apagada	Permite migrar una máquina virtual apagada a un grupo de recursos o host diferentes.	Máquinas virtuales	Resource.ColdMigrate
Migrar máquina virtual encendida	Permite migrar con vMotion una máquina virtual encendida a un grupo de recursos o host diferentes.	Máquinas virtuales	Resource.HotMigrate

Tabla 16-39. Privilegios de recursos (continuación)

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Modificar grupo de recursos	Permite cambiar las asignaciones de un grupo de recursos.	Grupos de recursos	Resource.EditPool
Mover grupo de recursos	Permite mover un grupo de recursos. El privilegio debe estar presente tanto en el origen como en el destino.	Grupos de recursos	Resource.MovePool
Consultar vMotion	Permite consultar la compatibilidad general de vMotion de una máquina virtual con un conjunto de hosts.	vCenter Server raíz	Resource.QueryVMotion
Quitar grupo de recursos	Permite eliminar un grupo de recursos. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	Grupos de recursos	Resource.DeletePool
Cambiar nombre de grupo de recursos	Permite cambiar el nombre a un grupo de recursos.	Grupos de recursos	Resource.RenamePool

Privilegios para tareas programadas

Estos privilegios controlan la creación, la edición y la eliminación de tareas programadas.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-40. Privilegios para tareas programadas

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Crear tareas	Permite programar una tarea. Se lo requiere, junto con los privilegios, para realizar la acción programada en el momento de la programación.	Cualquier objeto	ScheduledTask.Create
Modificar tarea	Permite volver a configurar las propiedades de la tarea programada.	Cualquier objeto	ScheduledTask.Edit
Quitar tarea	Permite quitar una tarea programada de la cola.	Cualquier objeto	ScheduledTask.Delete
Ejecutar tarea	Permite ejecutar la tarea programada de inmediato. Para crear y ejecutar una tarea programada también se necesitan permisos para la acción asociada.	Cualquier objeto	ScheduledTask.Run

Privilegios de sesiones

Los privilegios de sesiones controlan la capacidad de las extensiones para abrir sesiones en el sistema vCenter Server.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Nota Asigne privilegios de sesiones solo a administradores o usuarios de confianza.

Tabla 16-41. Privilegios de sesiones

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Suplantar usuario	Permite suplantar a otro usuario. Esta capacidad se utiliza con las extensiones.	vCenter Server raíz	Sessions.ImpersonateUser
Mensaje	Permite configurar el mensaje de inicio sesión global.	vCenter Server raíz	Sessions.GlobalMessage

Tabla 16-41. Privilegios de sesiones (continuación)

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Validar sesión	Permite verificar la validez de la sesión.	vCenter Server raíz	Sessions.ValidateSession
Ver y detener sesiones	Permite visualizar sesiones y forzar el cierre de sesión de uno o más usuarios conectados.	vCenter Server raíz	Sessions.TerminateSession
privilege.StorageProfile.ViewPermissions.label	Permite recopilar sesiones.	vCenter Server raíz	Sessions.CollectPrivilegeChecks

Privilegios de vistas de almacenamiento

Los privilegios de vistas de almacenamiento controlan los privilegios de las API de servicio de supervisión de almacenamiento.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-42. Privilegios de vistas de almacenamiento

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Configurar servicio	Permite a los usuarios con privilegios utilizar todas las API del servicio de supervisión de almacenamiento. Utilice **Vistas de almacenamiento.Ver** para los privilegios sobre las API de solo lectura del servicio de supervisión de almacenamiento.	vCenter Server raíz	StorageViews.ConfigureService
Ver	Permite a los usuarios con privilegios utilizar las API de solo lectura del servicio de supervisión de almacenamiento.	vCenter Server raíz	StorageViews.View

Privilegios de servicios de supervisor

Los privilegios de servicios de supervisor controlan quién puede crear y administrar servicios de supervisor en el entorno de vSphere with Tanzu.

Tabla 16-43. Privilegios de servicios de supervisor

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Administrar servicios de supervisor	Permite crear, actualizar o eliminar un servicio de supervisor. También permite instalar un servicio de supervisor en un clúster y crear o eliminar una versión del servicio de supervisor.	Clústeres	SupervisorServices.Manage

Privilegios de tareas

Los privilegios de tareas controlan la capacidad de las extensiones de crear y actualizar tareas en vCenter Server.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-44. Privilegios de tareas

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Crear tarea	Permite que una extensión cree una tarea definida por el usuario. Ninguno de los elementos de la interfaz de usuario de vSphere Client se asocia con este privilegio.	vCenter Server raíz	Task.Create
Actualizar tarea	Permite que una extensión actualice una tarea definida por el usuario. Ninguno de los elementos de la interfaz de usuario de vSphere Client se asocia con este privilegio.	vCenter Server raíz	Task.Update

Privilegios de administración de tenants

Los privilegios de administración de tenants controlan los aspectos de la definición y la recuperación de entidades de administración de tenants. (Se aplica a VMware Cloud on AWS).

Tabla 16-45. Privilegios de administración de tenants

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Operaciones de aprovisionamiento de tenants	Permite definir un conjunto de recursos que se utilizarán para la administración de tenants.	Carpeta raíz y cada entidad marcada actualmente como proveedor de servicios.	TenantManager.Update
Operaciones de consulta de tenants	Permite recuperar la lista de recursos de administración de tenants.	Carpeta raíz y cada entidad marcada actualmente como proveedor de servicios.	TenantManager.Query

Privilegios del servicio de transferencia

Los privilegios de servicio de transferencia son internos de VMware. No utilice estos privilegios.

Privilegios de VcTrusts/VcIdentity

Los privilegios de VcTrusts/VcIdentity controlan el acceso a diversas API internas y funciones relacionadas con la confianza entre sistemas vCenter Server.

Tabla 16-46. Privilegios de VcTrusts/VcIdentity

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Crear/Actualizar/Eliminar (privilegio de administradores)	Permite un acceso de nivel administrativo completo a varias API internas y funciones relacionadas con la confianza entre sistemas vCenter Server.	N/C	Trust.Administer
Crear/Actualizar/Eliminar (por debajo del privilegio de administradores)	Permite un acceso administrativo reducido a varias API internas y funciones relacionadas con la confianza entre sistemas vCenter Server. Este privilegio limita la creación, la actualización o la eliminación de VcTrusts/VcIdentity para que el usuario no pueda escalar privilegios que no son de administrador.	N/C	Trust.Manage

Privilegios de administrador de infraestructura de confianza

Los privilegios de administrador de infraestructura de confianza configuran y administran una implementación de vSphere Trust Authority.

Estos privilegios determinan quién puede realizar tareas de configuración y administración para una implementación de vSphere Trust Authority. Consulte Requisitos previos y privilegios necesarios para vSphere Trust Authority para obtener más información sobre las funciones de Trust Authority y el grupo de TrustedAdmins.

Tabla 16-47. Privilegios de administrador de infraestructura de confianza

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Configurar confianza de servidor de claves	Permite administrar los proveedores de claves del servicio de proveedor de claves.	vCenter Server raíz	TrustedAdmin.ManageKMSTrust
Configurar certificados TPM para el host de Trust Authority	Permite crear y modificar la configuración del servicio de atestación.	vCenter Server raíz	TrustedAdmin.ConfigureHostCertificates
Configurar metadatos para el host de Trust Authority	Permite editar las imágenes base que se atestarán mediante el servicio de atestación.	vCenter Server raíz	TrustedAdmin.ConfigureHostMetadata
Configurar SSO de atestación	Permite editar los hosts que pueden ser de confianza para los hosts de Trust Authority.	vCenter Server raíz	TrustedAdmin.ManageAttestingSSO
Configurar directiva de conversión de token	Permite configurar la directiva de conversión de tokens.	vCenter Server raíz	TrustedAdmin.ConfigureTokenConversionPolicy
Enumerar hosts de la infraestructura de confianza	Permite leer información sobre los hosts de confianza y los hosts de Trust Authority.	vCenter Server raíz	TrustedAdmin.ReadTrustedHosts

Tabla 16-47. Privilegios de administrador de infraestructura de confianza (continuación)

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Mostrar información sobre el STS	Permite exportar los detalles del host de confianza para que se puedan importar en el clúster de Trust Authority.	vCenter Server raíz	TrustedAdmin.ReadStsInfo
Administrar hosts de la infraestructura de confianza	Permite editar la información sobre los hosts de confianza y los hosts de Trust Authority.	vCenter Server raíz	TrustedAdmin.ManageTrustedHosts
Leer confianza de servidor de claves	Permite leer los proveedores de claves del servicio de proveedor de claves.	vCenter Server raíz	TrustedAdmin.ReadKMSTrust
Leer SSO de atestación	Permite leer los hosts de Trust Authority que pueden confiar en los hosts.	vCenter Server raíz	TrustedAdmin.ReadAttestingSSO
Recuperar certificados de TPM para el host de Trust Authority	Permite leer la configuración del servicio de atestación.	vCenter Server raíz	TrustedAdmin.RetrieveTPMHostCertificates
Recuperar metadatos para el host de Trust Authority	Permite leer las imágenes base que puede atestar el servicio de atestación.	vCenter Server raíz	TrustedAdmin.RetrieveHostMetadata

Privilegios de vApp

Los privilegios de vApp controlan las operaciones relacionadas con la implementación y la configuración de una vApp.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-48. Privilegios de vApp

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Agregar máquina virtual	Permite agregar una máquina virtual a una vApp.	vApps	VApp.AssignVM
Asignar grupo de recursos	Permite asignar un grupo de recursos a una vApp.	vApps	VApp.AssignResourcePool
Asignar vApp	Permite asignar una vApp a otra vApp.	vApps	VApp.AssignVApp
Clonar	Permite clonar una vApp.	vApps	VApp.Clone
Crear	Permite crear una vApp.	vApps	VApp.Create
Eliminar	Permite eliminar una vApp. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	vApps	VApp.Delete
Exportar	Permite exportar una vApp desde vSphere.	vApps	VApp.Export
Importar	Permite importar una vApp a vSphere.	vApps	VApp.Import
Mover	Permite mover una vApp a una nueva ubicación de inventario.	vApps	VApp.Move
Apagar	Permite apagar las operaciones en una vApp.	vApps	VApp.PowerOff
Encender	Permite encender las operaciones en una vApp.	vApps	VApp.PowerOn
Extraer de URL	Permite enumerar descriptores de archivos de origen remotos.	vApps	VApp.PullFromUrls
Cambiar nombre	Permite cambiarle el nombre a una vApp.	vApps	VApp.Rename
Suspender	Permite suspender una vApp.	vApps	VApp.Suspend

Tabla 16-48. Privilegios de vApp (continuación)

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Eliminar del registro	Permite anular el registro de una vApp. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	vApps	VApp.Unregister
Ver entorno de OVF	Permite visualizar el entorno de OVF de una máquina virtual encendida dentro de una vApp.	vApps	VApp.ExtractOvfEnvironment
Configuración de aplicaciones de vApp	Permite modificar la estructura interna de una vApp, como la información y las propiedades de un producto.	vApps	VApp.ApplicationConfig
Configuración de instancias de vApp	Permite modificar la configuración de las instancias de una vApp, como sus directivas.	vApps	VApp.InstanceConfig
Configuración de managedBy de vApp	Permite que una extensión o una solución marque una vApp como administrada por ella. Ninguno de los elementos de la interfaz de usuario de vSphere Client se asocia con este privilegio.	vApps	VApp.ManagedByConfig
Configuración de recursos de vApp	Permite modificar la configuración de recursos de una vApp. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	vApps	VApp.ResourceConfig

Privilegios de VcIdentityProviders

Los privilegios de VcIdentityProviders controlan el acceso a la API VcIdentityProviders.

Tabla 16-49. Privilegios de VcIdentityProviders

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Crear	Permite el acceso de solo creación a la API VcIdentityProviders (proveedores de identidad de vCenter Server).	N/C	VcIdentityProviders.Create
Administrar	Permite el acceso de escritura de nivel administrativo (crear, leer, actualizar y eliminar) a la API VcIdentityProviders (proveedores de identidad de vCenter Server).	N/C	VcIdentityProviders.Manage
Leer	Permite el acceso de lectura a la API VcIdentityProviders (proveedores de identidad de vCenter Server).	N/C	VcIdentityProviders.Read

Privilegios de configuración de VMware vSphere Lifecycle Manager

Los privilegios de configuración de VMware vSphere Lifecycle Manager controlan la capacidad de configurar el servicio vSphere Lifecycle Manager.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Nota Asigne privilegios que autoricen a los usuarios a invocar las API de VMware vSphere Lifecycle Manager que acepten direcciones URL solo para administradores o usuarios de confianza.

Tabla 16-50. Privilegios de configuración de VMware vSphere Lifecycle Manager

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
■ **Configurar** ■ **Configurar servicio**	Permite configurar el servicio vSphere Lifecycle Manager y la tarea programada de descarga de revisiones.	vCenter Server raíz	VcIntegrity.General.com.vmware.vcIntegrity.Configure

Privilegios de administración de configuración deseados de VMware vSphere Lifecycle Manager Manager

Los privilegios de administración de configuración deseados de VMware vSphere Lifecycle Manager controlan la capacidad de administrar la configuración de vSphere Lifecycle Manager.

Tabla 16-51. Privilegios de administración de configuración deseados de VMware vSphere Lifecycle Manager

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
■ **Privilegios de administración de configuración deseados** ■ **Exportar configuración de clúster deseada** ■ **Modificar configuración de clúster deseada** ■ **Acceso de solo lectura a la plataforma de administración de configuración deseada** ■ **Corregir el clúster según la configuración deseada**	**Exportar la configuración de clúster deseada** permite exportar la configuración o el esquema de configuración. **Modificar configuración de clúster deseada** permite importar una configuración o extraerla de un host de referencia. **Acceso de solo lectura a la plataforma de administración de configuración deseada** permite comprobar la conformidad, ejecutar la comprobación previa a la corrección y ver los resultados de la comprobación previa. **Corregir el clúster según la configuración deseada** permite corregir un clúster y realizar la transición a vSphere Configuration Profiles.	vCenter Server raíz	VcIntegrity.ClusterConfiguration.Export VcIntegrity.ClusterConfiguration.Modify VcIntegrity.ClusterConfiguration.View VcIntegrity.ClusterConfiguration.Remediate

Privilegios de perspectiva de estado de ESXi de VMware vSphere Lifecycle Manager

Los privilegios de perspectiva de estado de ESXi de VMware vSphere Lifecycle Manager controlan la capacidad de comprobar el estado de los hosts ESXi y de los clústeres.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-52. Privilegios de perspectiva de estado de ESXi de VMware vSphere Lifecycle Manager

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
■ **Perspectivas de estado de ESXi** ■ **Leer** ■ **Escribir**	**Leer** permite consultar el estado de los hosts ESXi y de los clústeres. **Escribir** no se utiliza actualmente.	Hosts Clústeres	VcIntegrity.lifecycleHealth.Read VcIntegrity.lifecycleHealth.Write

Privilegios de depósitos de VMware vSphere Lifecycle Manager

Los privilegios de depósitos de VMware vSphere Lifecycle Manager controlan la capacidad de administrar depósitos.

Tabla 16-53. Privilegios de depósitos de VMware vSphere Lifecycle Manager

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
■ **Lifecycle Manager: privilegios de depósitos** ■ **Eliminar**	Permite eliminar un almacén de vSphere Lifecycle Manager.	vCenter Server raíz	VcIntegrity.lifecycleDepots.Delete

Privilegios generales de VMware vSphere Lifecycle Manager

Los privilegios generales de VMware vSphere Lifecycle Manager controlan la capacidad de leer y escribir recursos de Lifecyle Manager.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-54. Privilegios generales de VMware vSphere Lifecycle Manager

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
■ **Lifecycle Manager: privilegios generales** ■ **Leer** ■ **Escribir**	**Leer** permite leer recursos de vSphere Lifecycle Manager. Este privilegio es necesario para obtener información de tareas. **Escribir** permite escribir recursos de vSphere Lifecycle Manager. Este privilegio es necesario para cancelar una tarea de vSphere Lifecycle Manager.	vCenter Server raíz	VcIntegrity.lifecycleGeneral.Read VcIntegrity.lifecycleGeneral.Write

Privilegios de compatibilidad de hardware de VMware vSphere Lifecycle Manager

Los privilegios de compatibilidad de hardware de VMware vSphere Lifecycle Manager controlan la capacidad de detectar y resolver posibles problemas de compatibilidad de hardware.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-55. Privilegios de compatibilidad de hardware de VMware vSphere Lifecycle Manager

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
■ **Lifecycle Manager: privilegios de compatibilidad de hardware** ■ **Acceder a compatibilidad de hardware** ■ **Escribir**	**Acceder a compatibilidad de hardware** Y **Escribir** permiten acceder a los datos de compatibilidad de hardware y resolver posibles problemas de compatibilidad de hardware.	Hosts	VcIntegrity.HardwareCompatibility.Read VcIntegrity.HardwareCompatibility.Write

Privilegios de imagen de VMware vSphere Lifecycle Manager

Los privilegios de imagen de VMware vSphere Lifecycle Manager controlan la capacidad de administrar imágenes.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Nota Asigne privilegios que autoricen a los usuarios a invocar las API de VMware vSphere Lifecycle Manager que acepten direcciones URL solo para administradores o usuarios de confianza.

Tabla 16-56. Privilegios de imagen de VMware vSphere Lifecycle Manager

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
■ **Lifecycle Manager: privilegios de imagen** ■ **Leer** ■ **Escribir**	**Leer** permite leer imágenes de vSphere Lifecycle Manager. Este privilegio es necesario para lo siguiente: ■ Mostrar todos los borradores de un clúster ■ Obtener más información sobre un borrador ■ Realizar una exploración en un borrador ■ Validar un borrador ■ Recuperar el contenido de un borrador ■ Calcular la lista de componentes efectivos ■ Obtiene el contenido del documento de estado deseado actual ■ Iniciar una exploración en un clúster ■ Obtener el resultado de cumplimiento ■ Obtener una recomendación ■ Exportar el estado deseado actual como un almacén, un archivo JSON o una imagen ISO **Escribir** permite administrar imágenes de vSphere Lifecycle Manager. Este privilegio es necesario para lo siguiente: ■ Crear, eliminar o confirmar un borrador ■ Importar el estado deseado ■ Generar recomendaciones ■ Establecer o eliminar distintas partes de un borrador	vCenter Server raíz	VcIntegrity.lifecycleSettings.Read VcIntegrity.lifecycleSettings.Write

Privilegios de corrección de imágenes de VMware vSphere Lifecycle Manager

Los privilegios de corrección de imágenes de VMware vSphere Lifecycle Manager controlan la capacidad de corregir imágenes.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-57. Privilegios de corrección de imágenes de VMware vSphere Lifecycle Manager

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
■ **Lifecycle Manager: privilegios de corrección de imágenes** ■ **Leer** ■ **Escribir**	**Leer** permite realizar la comprobación previa a la corrección. **Escribir** permite realizar la corrección.	Clústeres	VcIntegrity.lifecycleSoftwareRemediation.Read VcIntegrity.lifecycleSoftwareRemediation.Write

Privilegios de configuración de VMware vSphere Lifecycle Manager

Los privilegios de configuración de VMware vSphere Lifecycle Manager controlan la capacidad de administrar los almacenes y las directivas de corrección.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Nota Asigne privilegios que autoricen a los usuarios a invocar las API de VMware vSphere Lifecycle Manager que acepten direcciones URL solo para administradores o usuarios de confianza.

Tabla 16-58. Privilegios de configuración de VMware vSphere Lifecycle Manager

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
■ **Lifecycle Manager: privilegios de configuración** ■ **Leer** ■ **Escribir**	**Leer** permite leer almacenes y directivas de corrección de vSphere Lifecycle Manager. **Escribir** permite escribir almacenes y directivas de corrección de vSphere Lifecycle Manager.	vCenter Server raíz	VcIntegrity.lifecycleSoftwareSpecification.Read VcIntegrity.lifecycleSoftwareSpecification.Write

Privilegios de administración de líneas base de VMware vSphere Lifecycle Manager

Los privilegios de administración de líneas base de VMware vSphere Lifecycle Manager controlan la capacidad de administrar líneas base y grupos de líneas base.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-59. Privilegios de administración de líneas base de VMware vSphere Lifecycle Manager

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
■ **Administrar línea base** ■ **Asociar línea base** ■ **Administrar línea base**	**Asociar línea base** permite asociar líneas base y grupos de líneas base a objetos en el inventario de vSphere. **Administrar línea base** permite crear, editar o eliminar líneas base y grupos de líneas base.	vCenter Server raíz	VcIntegrity.Baseline.com.vmware.vcIntegrity.AssignBaselines VcIntegrity.Baseline.com.vmware.vcIntegrity.ManageBaselines

Privilegios de administración de revisiones y actualizaciones de VMware vSphere Lifecycle Manager

Los privilegios de administración de revisiones y actualizaciones de VMware vSphere Lifecycle Manager controlan la capacidad de ver, explorar y corregir revisiones, extensiones o actualizaciones aplicables.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-60. Privilegios de administración de revisiones y actualizaciones de VMware vSphere Lifecycle Manager

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
■ **Administrar revisiones y actualizaciones** ■ **Corregir para aplicar revisiones, extensiones y actualizaciones** ■ **Examinar en busca de revisiones, extensiones y actualizaciones correspondientes** ■ **Realizar copias intermedias de revisiones y extensiones** ■ **Ver estado de cumplimiento**	**Corregir para aplicar revisiones, extensiones y actualizaciones** permite la corrección de máquinas virtuales y hosts para aplicar revisiones, extensiones o actualizaciones cuando se utilizan líneas base. Este privilegio permite además ver el estado de cumplimiento. **Examinar en busca de revisiones, extensiones y actualizaciones correspondientes** permite examinar máquinas virtuales y hosts en busca de revisiones, extensiones o actualizaciones aplicables cuando se utilizan líneas base. **Realizar copias intermedias de revisiones y extensiones** permite realizar copias intermedias de revisiones o extensiones de hosts ESXi cuando se utilizan líneas base. Este privilegio permite además ver el estado de cumplimiento de los hosts ESXi. **Ver estado de cumplimiento** permite ver la información de cumplimiento de línea base de un objeto en el inventario de vSphere.	vCenter Server raíz	VcIntegrity.Updates.com.vmware.vcIntegrity.Remediate VcIntegrity.Updates.com.vmware.vcIntegrity.Scan VcIntegrity.Updates.com.vmware.vcIntegrity.Stage VcIntegrity.Updates.com.vmware.vcIntegrity.ViewStatus

Privilegios de carga de archivos de VMware vSphere Lifecycle Manager

Los privilegios de carga de archivos de VMware vSphere Lifecycle Manager controlan la capacidad de importar actualizaciones al almacén de vSphere Lifecycle Manager.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Nota Asigne privilegios que autoricen a los usuarios a invocar las API de VMware vSphere Lifecycle Manager que acepten direcciones URL solo para administradores o usuarios de confianza.

Tabla 16-61. Privilegios de carga de archivos de VMware vSphere Lifecycle Manager

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
■ **Cargar archivo** ■ **Cargar imágenes de actualización y paquetes sin conexión**	Permite cargar paquetes de revisiones sin conexión e ISO de actualización.	vCenter Server raíz	VcLifecycle.Upgrade

Privilegios de configuración de cambio de máquina virtual

Los privilegios de configuración de cambio de máquinas virtuales controlan la capacidad de configurar opciones y dispositivos de máquinas virtuales.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-62. Privilegios de configuración de cambio de máquina virtual

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
■ **Cambiar configuración** ■ **Adquirir concesión de discos**	Permite realizar operaciones de concesión de discos para una máquina virtual.	Máquinas virtuales	VirtualMachine.Config.DiskLease
■ **Cambiar configuración** ■ **Agregar un disco existente**	Permite agregar un disco virtual existente a una máquina virtual.	Máquinas virtuales	VirtualMachine.Config.AddExistingDisk
■ **Cambiar configuración** ■ **Agregar disco nuevo**	Permite crear un disco virtual nuevo para agregar a una máquina virtual.	Máquinas virtuales	VirtualMachine.Config.AddNewDisk

Tabla 16-62. Privilegios de configuración de cambio de máquina virtual (continuación)

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
■ **Cambiar configuración** ■ **Agregar o eliminar dispositivo**	Permite agregar o eliminar cualquier dispositivo que no sea un disco.	Máquinas virtuales	VirtualMachine.Config.AddRemoveDevice
■ **Cambiar configuración** ■ **Configuración avanzada**	Permite agregar o modificar parámetros avanzados en el archivo de configuración de la máquina virtual.	Máquinas virtuales	VirtualMachine.Config.AdvancedConfig
■ **Cambiar configuración** ■ **Cambiar recuento de CPU**	Permite cambiar la cantidad de CPU virtuales.	Máquinas virtuales	VirtualMachine.Config.CPUCount
■ **Cambiar configuración** ■ **Cambiar memoria**	Permite cambiar la cantidad de memoria asignada a la máquina virtual.	Máquinas virtuales	VirtualMachine.Config.Memory
■ **Cambiar configuración** ■ **Cambiar ajustes**	Permite cambiar la configuración general de la máquina virtual.	Máquinas virtuales	VirtualMachine.Config.Settings
■ **Cambiar configuración** ■ **Cambiar ubicación de archivo de intercambio**	Permite cambiar la directiva de selección del archivo de intercambio de una máquina virtual.	Máquinas virtuales	VirtualMachine.Config.SwapPlacement
■ **Cambiar configuración** ■ **Cambiar recurso**	Permite cambiar la configuración de recursos de un conjunto de nodos de máquinas virtuales en un grupo de recursos determinado.	Máquinas virtuales	VirtualMachine.Config.Resource
■ **Cambiar configuración** ■ **Configurar dispositivo USB de host**	Permite conectar un dispositivo USB basado en host a una máquina virtual.	Máquinas virtuales	VirtualMachine.Config.HostUSBDevice

Tabla 16-62. Privilegios de configuración de cambio de máquina virtual (continuación)

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
■ **Cambiar configuración** ■ **Configurar dispositivo sin formato**	Permite agregar y eliminar una asignación de discos sin formato o un dispositivo de acceso directo de SCSI. Al configurar este parámetro, se anula cualquier otro privilegio de modificación de dispositivos sin procesar, incluidos los estados de conexión.	Máquinas virtuales	VirtualMachine.Config.RawDevice
■ **Cambiar configuración** ■ **Configurar managedBy**	Permite que una extensión o solución marque una máquina virtual como administrada por ella.	Máquinas virtuales	VirtualMachine.Config.ManagedBy
■ **Cambiar configuración** ■ **Mostrar configuración de conexión**	Permite configurar opciones de consola remota de máquinas virtuales.	Máquinas virtuales	VirtualMachine.Config.MksControl
■ **Cambiar configuración** ■ **Extender disco virtual**	Permite expandir el tamaño de un disco virtual.	Máquinas virtuales	VirtualMachine.Config.DiskExtend
■ **Cambiar configuración** ■ **Modificar configuración de dispositivos**	Permite cambiar las propiedades de un dispositivo existente.	Máquinas virtuales	VirtualMachine.Config.EditDevice
■ **Cambiar configuración** ■ **Consultar compatibilidad con Fault Tolerance**	Permite comprobar si una máquina virtual es compatible con Fault Tolerance.	Máquinas virtuales	VirtualMachine.Config.QueryFTCompatibility

Tabla 16-62. Privilegios de configuración de cambio de máquina virtual (continuación)

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
■ **Cambiar configuración** ■ **Consultar archivos sin propietario**	Permite consultar archivos sin propietario.	Máquinas virtuales	VirtualMachine.Config.QueryUnownedFiles
■ **Cambiar configuración** ■ **Volver a cargar desde la ruta de acceso**	Permite cambiar la ruta de acceso de configuración de una máquina virtual y, a la vez, preservar la identidad de esta última. Las soluciones como vCenter Site Recovery Manager de VMware usan esta operación para resguardar la identidad de la máquina virtual durante la conmutación por error y la conmutación por recuperación.	Máquinas virtuales	VirtualMachine.Config.ReloadFromPath
■ **Cambiar configuración** ■ **Eliminar disco**	Permite extraer el dispositivo de disco virtual.	Máquinas virtuales	VirtualMachine.Config.RemoveDisk
■ **Cambiar configuración** ■ **Cambiar nombre**	Permite cambiar el nombre de una máquina virtual o modificar las notas asociadas de una máquina virtual.	Máquinas virtuales	VirtualMachine.Config.Rename
■ **Cambiar configuración** ■ **Restablecer información del invitado**	Permite editar la información de sistemas operativos invitados de una máquina virtual.	Máquinas virtuales	VirtualMachine.Config.ResetGuestInfo
■ **Cambiar configuración** ■ **Configurar anotación**	Permite agregar o editar una anotación de máquina virtual.	Máquinas virtuales	VirtualMachine.Config.Annotation

Tabla 16-62. Privilegios de configuración de cambio de máquina virtual (continuación)

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
■ **Cambiar configuración** ■ **Alternar seguimiento de cambios del disco**	Permite activar o desactivar el seguimiento de cambios para los discos de la máquina virtual.	Máquinas virtuales	VirtualMachine.Config.ChangeTracking
■ **Cambiar configuración** ■ **Alternar elemento primario de bifurcación**	Permite activar o desactivar un elemento principal de vmfork.	Máquinas virtuales	VirtualMachine.Config.ToggleForkParent
■ **Cambiar configuración** ■ **Actualizar compatibilidad de la máquina virtual**	Permite actualizar la versión de compatibilidad de la máquina virtual.	Máquinas virtuales	VirtualMachine.Config.UpgradeVirtualHardware

Privilegios de operaciones de invitado de máquina virtual

Los privilegios de operaciones de invitado de máquina virtual controlan la capacidad de interacción con archivos y aplicaciones que se encuentran en el sistema operativo invitado de una máquina virtual con la API.

Consulte la documentación sobre la *Referencia de vSphere Web Services API* para obtener más información sobre dichas operaciones.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-63. Operaciones de invitado de la máquina virtual

Nombre del privilegio en vSphere Client	Descripción	Efectivo en el objeto	Nombre de privilegio en la API
■ **Operaciones de invitado** ■ **Modificación de alias de operaciones de invitado**	Permite las operaciones de invitado de máquina virtual que implican modificar el alias de la máquina virtual.	Máquinas virtuales	VirtualMachine.GuestOperations.ModifyAliases
■ **Operaciones de invitado** ■ **Consulta de alias de operaciones de invitado**	Permite las operaciones de invitado de máquina virtual que implican consultar el alias de la máquina virtual.	Máquinas virtuales	VirtualMachine.GuestOperations.QueryAliases
■ **Operaciones de invitado** ■ **Modificaciones de operaciones de invitado**	Permite las operaciones de invitado de máquina virtual que implican modificaciones en un sistema operativo invitado de una máquina virtual, como la transferencia de un archivo a la máquina virtual. Ninguno de los elementos de la interfaz de usuario de vSphere Client se asocia con este privilegio.	Máquinas virtuales	VirtualMachine.GuestOperations.Modify

Tabla 16-63. Operaciones de invitado de la máquina virtual (continuación)

Nombre del privilegio en vSphere Client	Descripción	Efectivo en el objeto	Nombre de privilegio en la API
■ **Operaciones de invitado** ■ **Ejecución de programas de operaciones de invitado**	Permite operaciones de invitado de máquina virtual que implican la ejecución de una aplicación en la máquina virtual. Ninguno de los elementos de la interfaz de usuario de vSphere Client se asocia con este privilegio.	Máquinas virtuales	VirtualMachine.GuestOperations.Execute
■ **Operaciones de invitado** ■ **Consultas de operaciones de invitado**	Permite las operaciones de invitado de máquina virtual que implican consultar el sistema operativo invitado, como enumerar archivos en el sistema operativo invitado. Ninguno de los elementos de la interfaz de usuario de vSphere Client se asocia con este privilegio.	Máquinas virtuales	VirtualMachine.GuestOperations.Query

Privilegios para la interacción con máquinas virtuales

Estos privilegios controlan la capacidad de interactuar con la consola de una máquina virtual, configurar soportes físicos, realizar operaciones de energía e instalar VMware Tools.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-64. Interacción con la máquina virtual

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
■ **Interacción** ■ **Answer question**	Permite solucionar problemas con las transiciones de estados de las máquinas virtuales o con errores de tiempo de ejecución.	Máquinas virtuales	VirtualMachine.Interact.AnswerQuestion
■ **Interacción** ■ **Backup operation on virtual machine**	Permite realizar operaciones de copia de seguridad en las máquinas virtuales.	Máquinas virtuales	VirtualMachine.Interact.Backup
■ **Interacción** ■ **Configurar medio de CD**	Permite configurar un dispositivo virtual de DVD o CD-ROM.	Máquinas virtuales	VirtualMachine.Interact.SetCDMedia
■ **Interacción** ■ **Configurar medio de disquete**	Permite configurar un dispositivo virtual de disquete.	Máquinas virtuales	VirtualMachine.Interact.SetFloppyMedia
■ **Interacción** ■ **Console interaction**	Permite interactuar con el mouse, el teclado y la pantalla virtuales de las máquinas virtuales.	Máquinas virtuales	VirtualMachine.Interact.ConsoleInteract
■ **Interacción** ■ **Create screenshot**	Permite crear una captura de pantalla de una máquina virtual.	Máquinas virtuales	VirtualMachine.Interact.CreateScreenshot
■ **Interacción** ■ **Defragment all disks**	Permite realizar operaciones de desfragmentación en todos los discos de la máquina virtual.	Máquinas virtuales	VirtualMachine.Interact.DefragmentAllDisks
■ **Interacción** ■ **Device connection**	Permite cambiar el estado conectado de los dispositivos virtuales desconectables de una máquina virtual.	Máquinas virtuales	VirtualMachine.Interact.DeviceConnection
■ **Interacción** ■ **Drag and Drop**	Permite arrastrar y soltar archivos entre una máquina virtual y un cliente remoto.	Máquinas virtuales	VirtualMachine.Interact.DnD

Tabla 16-64. Interacción con la máquina virtual (continuación)

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
■ **Interacción** ■ **Guest operating system management by VIX API**	Permite administrar el sistema operativo de la máquina virtual mediante VIX API.	Máquinas virtuales	VirtualMachine.Interact.GuestControl
■ **Interacción** ■ **Inject USB HID scan codes**	Permite inyectar códigos de análisis de dispositivos USB HID.	Máquinas virtuales	VirtualMachine.Interact.PutUsbScanCodes
■ **Interacción** ■ **Pausar o cancelar la pausa**	Permite poner en pausa la máquina virtual y anular la pausa.	Máquinas virtuales	VirtualMachine.Interact.Pause
■ **Interacción** ■ **Perform wipe or shrink operations**	Permite realizar operaciones de borrado o reducción en la máquina virtual.	Máquinas virtuales	VirtualMachine.Interact.SESparseMaintenance
■ **Interacción** ■ **Power Off**	Permite apagar una máquina virtual que se encuentra encendida. Esta operación apaga el sistema operativo invitado.	Máquinas virtuales	VirtualMachine.Interact.PowerOff
■ **Interacción** ■ **Power On**	Permite encender una máquina virtual que se encuentra apagada y reanudar una máquina virtual suspendida.	Máquinas virtuales	VirtualMachine.Interact.PowerOn
■ **Interacción** ■ **Record session on Virtual Machine**	Permite grabar una sesión en una máquina virtual.	Máquinas virtuales	VirtualMachine.Interact.Record
■ **Interacción** ■ **Replay session on Virtual Machine**	Permite reproducir una sesión grabada en una máquina virtual.	Máquinas virtuales	VirtualMachine.Interact.Replay
■ **Interacción** ■ **Reset**	Permite restablecer una máquina virtual y reiniciar el sistema operativo invitado.	Máquinas virtuales	VirtualMachine.Interact.Reset

Tabla 16-64. Interacción con la máquina virtual (continuación)

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
■ **Interacción** ■ **Reanudar Fault Tolerance**	Permite reanudar la tolerancia a errores en una máquina virtual.	Máquinas virtuales	VirtualMachine.Interact.EnableSecondary
■ **Interacción** ■ **Suspend**	Permite suspender una máquina virtual que se encuentra encendida. Esta operación pone al invitado en modo de espera.	Máquinas virtuales	VirtualMachine.Interact.Suspend
■ **Interacción** ■ **Suspender Fault Tolerance**	Permite suspender la tolerancia a errores en una máquina virtual.	Máquinas virtuales	VirtualMachine.Interact.DisableSecondary
■ **Interacción** ■ **Suspender en la memoria**	Permite suspender la memoria de una máquina virtual.	Máquinas virtuales	VirtualMachine.Interact.SuspendToMemory
■ **Interacción** ■ **Test failover**	Permite probar la conmutación por error de Fault Tolerance al convertir la máquina virtual secundaria en la máquina virtual principal.	Máquinas virtuales	VirtualMachine.Interact.MakePrimary
■ **Interacción** ■ **Test restart Secondary VM**	Permite finalizar la máquina virtual secundaria de una máquina virtual mediante Fault Tolerance.	Máquinas virtuales	VirtualMachine.Interact.DisableSecondary
■ **Interacción** ■ **Turn Off Fault Tolerance**	Permite apagar Fault Tolerance en una máquina virtual.	Máquinas virtuales	VirtualMachine.Interact.TurnOffFaultTolerance
■ **Interacción** ■ **Turn On Fault Tolerance**	Permite encender Fault Tolerance en una máquina virtual.	Máquinas virtuales	VirtualMachine.Interact.CreateSecondary
■ **Interacción** ■ **VMware Tools install**	Permite montar y desmontar el CD instalador de VMware Tools como CD-ROM del sistema operativo invitado.	Máquinas virtuales	VirtualMachine.Interact.ToolsInstall

Privilegios de edición de inventario de máquinas virtuales

Los privilegios de edición de inventario de máquinas virtuales controlan las operaciones de adición, movimiento y eliminación de máquinas virtuales.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-65. Privilegios de edición de inventario de máquinas virtuales

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
■ **Editar el inventario** ■ **Crear a partir de existente**	Permite crear una máquina virtual a partir de una máquina virtual o plantilla existentes, mediante la clonación o la implementación desde una plantilla.	Clústeres, hosts, carpetas de máquina virtual	VirtualMachine.Inventory.CreateFromExisting
■ **Editar el inventario** ■ **Crear nuevo**	Permite crear una máquina virtual y asignar recursos para su ejecución.	Clústeres, hosts, carpetas de máquina virtual	VirtualMachine.Inventory.Create
■ **Editar el inventario** ■ **Mover**	Permite mover de lugar una máquina virtual en la jerarquía. El privilegio debe estar presente tanto en el origen como en el destino.	Máquinas virtuales	VirtualMachine.Inventory.Move
■ **Editar el inventario** ■ **Registrar**	Permite agregar una máquina virtual existente a vCenter Server o al inventario de hosts.	Clústeres, hosts, carpetas de máquina virtual	VirtualMachine.Inventory.Register

Tabla 16-65. Privilegios de edición de inventario de máquinas virtuales (continuación)

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
■ **Editar el inventario** ■ **Eliminar**	Permite eliminar una máquina virtual. Esta acción elimina del disco los archivos subyacentes de la máquina virtual. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	Máquinas virtuales	VirtualMachine.Inventory.Delete
■ **Editar el inventario** ■ **Cancelar el registro**	Permite cancelar el registro de una máquina virtual de una instancia de vCenter Server o un inventario de host. Para tener los permisos necesarios para realizar esta operación, un usuario o un grupo deben tener este privilegio asignado tanto en el objeto como en su objeto primario.	Máquinas virtuales	VirtualMachine.Inventory.Unregister

Privilegios de aprovisionamiento de las máquinas virtuales

Los privilegios de aprovisionamiento de las máquinas virtuales controlan las actividades relacionadas con la implementación y la personalización de las máquinas virtuales.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-66. Privilegios de aprovisionamiento de las máquinas virtuales

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
■ **Provisioning** ■ **Allow disk access**	Permite abrir un disco en una máquina virtual con acceso aleatorio de lectura y escritura. Se utiliza sobre todo para el montaje de discos remotos.	Máquinas virtuales	VirtualMachine.Provisioning.DiskRandomAccess
■ **Aprovisionamiento** ■ **Permitir acceso a archivos**	Permite operaciones en archivos asociados con una máquina virtual, incluido vmx, discos, registros y nvram.	Máquinas virtuales	VirtualMachine.Provisioning.FileRandomAccess
■ **Provisioning** ■ **Allow read-only disk access**	Permite abrir un disco en una máquina virtual con acceso aleatorio de lectura. Se utiliza sobre todo para el montaje de discos remotos.	Máquinas virtuales	VirtualMachine.Provisioning.DiskRandomRead
■ **Provisioning** ■ **Allow virtual machine download**	Permite leer operaciones en archivos asociados con una máquina virtual, incluido vmx, discos, registros y nvram.	Host raíz o vCenter Server	VirtualMachine.Provisioning.GetVmFiles
■ **Provisioning** ■ **Allow virtual machine files upload**	Permite escribir operaciones en archivos asociados con una máquina virtual, incluido vmx, discos, registros y nvram.	Host raíz o vCenter Server	VirtualMachine.Provisioning.PutVmFiles

Tabla 16-66. Privilegios de aprovisionamiento de las máquinas virtuales (continuación)

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
■ **Provisioning** ■ **Clone template**	Permite clonar una plantilla.	Plantillas	VirtualMachine.Provisioning.CloneTemplate
■ **Provisioning** ■ **Clone virtual machine**	Permite clonar una máquina virtual ya existente y asignar recursos.	Máquinas virtuales	VirtualMachine.Provisioning.Clone
■ **Provisioning** ■ **Create template from virtual machine**	Permite crear una plantilla nueva desde una máquina virtual.	Máquinas virtuales	VirtualMachine.Provisioning.CreateTemplateFromVM
■ **Aprovisionamiento** ■ **Personalizar invitado**	Permite personalizar el sistema operativo invitado de una máquina virtual sin moverla.	Máquinas virtuales	VirtualMachine.Provisioning.Customize
■ **Provisioning** ■ **Deploy template**	Permite implementar una máquina virtual desde una plantilla.	Plantillas	VirtualMachine.Provisioning.DeployTemplate
■ **Provisioning** ■ **Mark as template**	Permite marcar como una plantilla a una máquina virtual ya existente que está apagada.	Máquinas virtuales	VirtualMachine.Provisioning.MarkAsTemplate
■ **Provisioning** ■ **Mark as virtual machine**	Permite marcar una plantilla existente como una máquina virtual.	Plantillas	VirtualMachine.Provisioning.MarkAsVM
■ **Provisioning** ■ **Modify customization specification**	Permite crear, modificar o eliminar especificaciones de personalización.	vCenter Server raíz	VirtualMachine.Provisioning.ModifyCustSpecs

Tabla 16-66. Privilegios de aprovisionamiento de las máquinas virtuales (continuación)

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
■ **Provisioning** ■ **Promote disks**	Permite promover operaciones en los discos de una máquina virtual.	Máquinas virtuales	VirtualMachine.Provisioning.PromoteDisks
■ **Provisioning** ■ **Read customization specifications**	Permite leer una especificación de personalización.	Máquinas virtuales	VirtualMachine.Provisioning.ReadCustSpecs

Privilegios de configuración de servicios de la máquina virtual

Los privilegios de configuración de servicios de la máquina virtual controlan quién puede realizar tareas de supervisión y administración en la configuración de servicios.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-67. Privilegios de configuración de servicios de la máquina virtual

Nombre del privilegio en vSphere Client	Descripción	Nombre de privilegio en la API
■ **Configuración de servicios** ■ **Permitir notificaciones**	Permite generar y recibir notificaciones sobre el estado del servicio.	VirtualMachine.Namespace.Event
■ **Configuración de servicios** ■ **Permitir medición de notificaciones de eventos globales**	Permite consultar si hay notificaciones presentes.	VirtualMachine.Namespace.EventNotify
■ **Configuración de servicios** ■ **Administrar configuración de servicios**	Permite crear, modificar y eliminar servicios de la máquina virtual.	VirtualMachine.Namespace.Management
■ **Configuración de servicios** ■ **Modificar configuración de servicios**	Permite modificar la configuración actual del servicio de la máquina virtual.	VirtualMachine.Namespace.ModifyContent

Tabla 16-67. Privilegios de configuración de servicios de la máquina virtual (continuación)

Nombre del privilegio en vSphere Client	Descripción	Nombre de privilegio en la API
■ **Configuración de servicios** ■ **Consultar configuración de servicios**	Permite recuperar la lista de servicios de la máquina virtual.	VirtualMachine.Namespace.Query
■ **Configuración de servicios** ■ **Leer configuración de servicios**	Permite recuperar la configuración actual del servicio de la máquina virtual.	VirtualMachine.Namespace.ReadContent

Privilegios de administración de snapshots de las máquinas virtuales

Los privilegios de administración de snapshots de las máquinas virtuales controlan la capacidad para crear, eliminar, cambiar el nombre y restaurar snapshots.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-68. Privilegios de administración de snapshots de las máquinas virtuales

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
■ **Administración de instantáneas** ■ **Crear instantánea**	Permite crear una snapshot a partir del estado actual de la máquina virtual.	Máquinas virtuales	VirtualMachine.State.CreateSnapshot
■ **Snapshot management** ■ **Remove Snapshot**	Permite quitar una snapshot del historial de snapshots.	Máquinas virtuales	VirtualMachine.State.RemoveSnapshot
■ **Snapshot management** ■ **Rename Snapshot**	Permite cambiar el nombre de una snapshot con un nuevo nombre, una nueva descripción o ambos.	Máquinas virtuales	VirtualMachine.State.RenameSnapshot
■ **Snapshot management** ■ **Revert to snapshot**	Permite configurar la máquina virtual con el estado que tenía en una snapshot determinada.	Máquinas virtuales	VirtualMachine.State.RevertToSnapshot

Privilegios de vSphere Replication de máquinas virtuales

Los privilegios de vSphere Replication de máquinas virtuales controlan la utilización de la replicación que hace VMware vCenter Site Recovery Manager™ en máquinas virtuales.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-69. Privilegios de vSphere Replication de máquinas virtuales

Nombre de privilegio en	Descripción	Necesario para	Nombre de privilegio en la API
■ **vSphere Replication** ■ **Configurar replicación**	Permite configurar la replicación de la máquina virtual.	Máquinas virtuales	VirtualMachine.Hbr.ConfigureReplication
■ **vSphere Replication** ■ **Administrar replicación**	Permite activar la sincronización completa, en línea o sin conexión de una replicación.	Máquinas virtuales	VirtualMachine.Hbr.ReplicaManagement
■ **vSphere Replication** ■ **Supervisar replicación**	Permite supervisar la replicación.	Máquinas virtuales	VirtualMachine.Hbr.MonitorReplication

Privilegios de clases de máquinas virtuales

Los privilegios de clases de máquinas virtuales controlan quién puede agregar y eliminar clases de máquinas virtuales en un espacio de nombres de Kubernetes.

Tabla 16-70. Privilegios de clases de máquinas virtuales

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Administrar clases de máquinas virtuales	Permite administrar clases de máquinas virtuales en espacios de nombres de Kubernetes en un clúster supervisor.	Clústeres	VirtualMachineClasses.Manage

Privilegios de vSAN

Los privilegios de vSAN controlan quién puede realizar operaciones de regeneración de claves superficial y actualizar la información del cliente.

Tabla 16-71. Privilegios de vSAN

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
■ **Clúster** ■ **ShallowRekey**	Permite realizar una regeneración de claves superficiales para un clúster.	Clústeres	Vsan.Cluster.ShallowRekey
■ **Xvc** ■ **UpdateClientInfo**	Se utiliza internamente.	Usuario de servicio	Vsan.Xvc.UpdateClientInfo

Privilegios de estadísticas de vSAN

Los privilegios de estadísticas de vSphere controlan la capacidad de acceder a las métricas de vSAN.

Tabla 16-72. Privilegios de estadísticas de vSAN

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Acceder al endpoint de detección de servicios de estadísticas de vSAN	Permite acceder al endpoint de detección de servicios `https://`*vCenterServer-IP* `/vsan/metrics/serviceDiscovery`.	Función de la cuenta de servicio.	vSANStats.Access

Privilegios de zonas de vSphere

Los privilegios de zonas de vSphere controlan quién puede crear y administrar zonas de vSphere en vSphere with Tanzu.

Tabla 16-73. Privilegios de zonas de vSphere

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Asociar y desasociar objetos de vSphere para zonas de vSphere	Permite asociar objetos con una zona de vSphere.	Clústeres	Zone.ObjectAttachable
Crear, actualizar y eliminar zonas de vSphere y sus asociaciones	Permite crear y eliminar una zona de vSphere.	Clústeres	Zone.Manage

Privilegios de vService

Los privilegios de vService controlan la capacidad de crear, configurar y actualizar dependencias de vService para máquinas virtuales y vApps.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-74. Privilegios de vService

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Crear dependencia	Permite crear una dependencia de vService para una máquina virtual o vApp.	vApps y máquinas virtuales	vService.CreateDependency
Destruir dependencia	Permite quitar una dependencia de vService para una máquina virtual o vApp.	vApps y máquinas virtuales	vService.DestroyDependency
Volver a ajustar la configuración de dependencia	Permite volver a configurar una dependencia para actualizar el proveedor o la unión.	vApps y máquinas virtuales	vService.ReconfigureDependency
Actualizar dependencia	Permite actualizar una dependencia para configurar el nombre o la descripción.	vApps y máquinas virtuales	vService.UpdateDependency

Privilegios de etiquetado de vSphere

Los privilegios de etiquetado de vSphere controlan la capacidad de crear y eliminar etiquetas y categorías de etiquetas, así como de asignar y quitar etiquetas en los objetos de inventario de vCenter Server.

Se puede establecer este privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Tabla 16-75. Privilegios de etiquetado de vSphere

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Asignar o desasignar etiqueta de vSphere	Permite asignar o anular la asignación de una etiqueta de un objeto en el inventario de vCenter Server.	Cualquier objeto	InventoryService.Tagging.AttachTag
Asignar una etiqueta de vSphere en un objeto o anular dicha asignación	Permite que a los objetos se les asignen etiquetas o se anule la asignación de etiquetas de ellos. Utilice este privilegio para limitar los objetos a los que los usuarios pueden asignar etiquetas o de los que pueden anular la asignación de etiquetas.	Cualquier objeto	InventoryService.Tagging.ObjectAttachable
Crear etiqueta de vSphere	Permite crear una etiqueta.	Cualquier objeto	InventoryService.Tagging.CreateTag
Crear categoría de etiqueta de vSphere	Permite crear una categoría de etiqueta.	Cualquier objeto	InventoryService.Tagging.CreateCategory
Eliminar etiqueta de vSphere	Permite eliminar una etiqueta.	Cualquier objeto	InventoryService.Tagging.DeleteTag
Eliminar categoría de etiqueta de vSphere	Permite eliminar una etiqueta.	Cualquier objeto	InventoryService.Tagging.DeleteCategory
Editar etiqueta de vSphere	Permite editar una etiqueta.	Cualquier objeto	InventoryService.Tagging.EditTag
Editar categoría de etiqueta de vSphere	Permite editar una categoría de etiqueta.	Cualquier objeto	InventoryService.Tagging.EditCategory
Modificar campo UsedBy por categoría	Permite cambiar el campo Usado por en una categoría de etiqueta.	Cualquier objeto	InventoryService.Tagging.ModifyUsedByForCategory
Modificar campo UsedBy por etiqueta	Permite cambiar el campo Usado por de una etiqueta.	Cualquier objeto	InventoryService.Tagging.ModifyUsedByForTag

Privilegios de vSphere Client

los privilegios de vSphere Client controlan el acceso sin conexión a vCenter Server.

Estos privilegios se aplican solo a VMware Cloud.

Privilegios de vSphere Data Protection

Los privilegios de vSphere Data Protection controlan la capacidad de administrar la solución de copia de seguridad y recuperación VMware vSphere® Data Protection™.

Tabla 16-76. Privilegios de vSphere Data Protection

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Protección	Permite realizar operaciones de protección de datos, como crear y administrar copias de seguridad.	vCenter Server	vSphereDataProtection.Protection
Recuperación	Permite realizar operaciones de protección de datos, como restaurar copias de seguridad.	vCenter Server	vSphereDataProtection.Recovery

Privilegios de estadísticas de vSphere

Los privilegios de estadísticas de vSphere controlan la capacidad de acceder al estado de vStats y a los datos de estadísticas en objetos como máquinas virtuales y hosts.

Tabla 16-77. Privilegios de estadísticas de vSphere

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Recopilar datos de estadísticas	Permite crear y actualizar especificaciones de adquisición en vStats.	El objeto para el que se recopilan los datos de estadísticas.	vStats.CollectAny
Modificar configuración de estadísticas	Permite administrar las opciones de configuración del servicio de vStats.	vCenter Server	vStats.Configuración
Consultar datos de estadísticas	Permite enumerar proveedores de estadísticas, métricas y contadores que exponen los proveedores, para los cuales los proveedores pueden recopilar datos de estadísticas.	El objeto para el que se consultan los datos de estadísticas.	vStats.QueryAny

Fortalecimiento y conformidad de vSphere

17

Se espera que las organizaciones reduzcan el riesgo de robo de datos, ataque cibernético o acceso no autorizado para proteger sus datos. Además, las organizaciones deben cumplir con los reglamentos de las normas gubernamentales y las normas privadas, como el Instituto nacional de normas y tecnología (National Institute of Standards and Technology, NIST) y las Guías de implementación técnica de seguridad (Security Technical Implementation Guides, STIG) de la Agencia de sistemas de información de defensa (Defense Information Systems Agency, DISA). Garantizar la conformidad de un entorno de vSphere con estas normas implica comprender un conjunto más amplio de consideraciones, incluidas personas, procesos y tecnología.

Una descripción general detallada de los temas de seguridad y conformidad que requieren atención permite planificar la estrategia de seguridad. También se pueden aprovechar otros recursos relacionados con la conformidad disponibles en el sitio web de VMware.

Lea los siguientes temas a continuación:

Seguridad y conformidad en el entorno de vSphere

Generalmente, los términos "seguridad" y "conformidad" se utilizan como sinónimos. Sin embargo, son conceptos únicos y distintos.

La seguridad, que normalmente se piensa como seguridad de la información, se define como un conjunto de controles técnicos, físicos y administrativos que se implementan para proporcionar confidencialidad, integridad y disponibilidad. Por ejemplo, para proteger un host, se bloquean las cuentas que pueden iniciar sesión en el host y el medio por el cual pueden hacerlo (SSH, consola directa, etc.). La conformidad, por el contrario, es un conjunto de requisitos necesarios para cumplir con los controles mínimo establecidos por diferentes marcos normativos en los que se proporcionan directrices limitadas sobre un tipo específico de tecnología, proveedor o configuración. Por ejemplo, la industria de tarjetas de pago (Payment Card Industry, PCI) establece directrices de seguridad para ayudar a las organizaciones a proteger proactivamente los datos de las cuentas de clientes.

La seguridad reduce el riesgo de robo de datos, ataque cibernético o acceso no autorizado, mientras que la conformidad es la prueba de que un control de seguridad está en vigor, por lo general, dentro de una línea de tiempo definida. La seguridad se expone principalmente en las decisiones de diseño y se destaca dentro de las configuraciones de tecnología. La conformidad se centra en trazar la correlación entre los controles de seguridad y los requisitos específicos. Un mapa de conformidad proporciona una vista centralizada para enumerar muchos de los controles de seguridad requeridos. Esos controles se describen más detalladamente cuando se incluyen las respectivas citas de conformidad de cada control de seguridad según lo indica un dominio como NIST, PCI, FedRAMP, HIPAA, etc.

Los programas efectivos de conformidad y ciberseguridad se basan en tres pilares: personas, procesos y tecnología. Un error de concepto general es que solo la tecnología puede resolver todas las necesidades de ciberseguridad. La tecnología desempeña un papel importante y amplio en el desarrollo y la ejecución de un programa de seguridad de la información. Sin embargo, si la tecnología no cuenta con procesos ni procedimientos, conocimientos ni formación, genera una vulnerabilidad dentro de la organización.

Al definir las estrategias de seguridad y conformidad, tenga en cuenta lo siguiente:

- Las personas necesitan formación y conocimientos generales, mientras que el personal de TI necesita formación específica.
- El proceso define cómo se utilizan las actividades, las funciones y la documentación dentro de una organización para mitigar los riesgos. Los procesos solo son efectivos si las personas los siguen correctamente.
- La tecnología puede utilizarse para prevenir o reducir el impacto de los riesgos de ciberseguridad sobre la organización. Qué tecnología se utilizará depende del nivel de aceptación de riesgos dentro de una organización.

VMware proporciona kits de conformidad que contienen una guía de auditoría y una guía de aplicabilidad de productos, lo que ayuda a puentear la brecha entre los requisitos de conformidad y normativas y las guías de implementación. Para obtener más información, consulte https://core.vmware.com/compliance.

Glosario de términos de conformidad

La conformidad introduce términos y definiciones específicos que es importante comprender.

Tabla 17-1. Términos de conformidad

Término	Definición
CJIS	Servicios de información de justicia penal. En el contexto de la conformidad, CJIS desarrolla una directiva de seguridad sobre la forma en que la justicia penal local, estatal y federal y los organismos de seguridad deben tomar precauciones de seguridad para proteger la información confidencial, como las huellas digitales y los antecedentes penales.
STIG de DISA	Guía de implementación técnica de seguridad de la Agencia de sistemas de información de defensa. La Agencia de Sistemas de Información de Defensa (Defense Information Systems Agency, DISA) es la entidad responsable de mantener la posición de seguridad de la infraestructura de TI del Departamento de Defensa (Department of Defense, DoD). DISA lleva a cabo esta tarea mediante el desarrollo y el uso de guías de implementación técnica de seguridad (Security Technical Implementation Guides, STIG).
FedRAMP	Programa federal de administración de riesgos y autorizaciones. FedRAMP es un programa gubernamental con un enfoque estandarizado para la evaluación, la autorización y la supervisión continua de la seguridad de los productos y servicios de nube.
HIPAA	Ley de transferencia y responsabilidad de seguro médico. Aprobada en el congreso en 1996, la ley HIPAA hace lo siguiente: ■ Otorga a millones de trabajadores norteamericanos y sus familias la capacidad de transferir y continuar con la cobertura de seguro médico cuando cambian su trabajo o lo pierden. ■ Reduce los fraudes y los abusos en atención médica. ■ Impone normas para todo el sector sobre la información de atención médica en la facturación electrónica y otros procesos. ■ Requiere la protección y la manipulación confidencial de la información de salud protegida. La última viñeta es de máxima importancia para la documentación *Seguridad de vSphere*.
NCCoE	Centro Nacional de Excelencia en Ciberseguridad. NCCoE es una organización gubernamental de Estados Unidos que produce y comparte públicamente soluciones para los problemas de ciberseguridad que padecen las empresas norteamericanas. El centro forma un equipo con personal de empresas de tecnología de ciberseguridad, otros organismos federales y la comunidad académica para abordar cada problema.

Tabla 17-1. Términos de conformidad (continuación)

Término	Definición
NIST	Instituto nacional de normas y tecnología. Fundado en 1901, el NIST es un organismo federal no regulador dentro del Departamento de comercio de Estados Unidos. La misión de NIST es fomentar la innovación y la competitividad industrial de Estados Unidos mediante la promoción de normas, tecnologías y ciencias de la medición con el fin de aumentar la seguridad económica y mejorar nuestra calidad de vida.
PAG	Guía de aplicabilidad de productos. Este documento proporciona directrices generales para las organizaciones que están considerando usar soluciones de una empresa con el fin de abordar sus requisitos de conformidad.
DSS de PCI	Estándar de seguridad de datos para la Industria de tarjeta de pago. Un conjunto de normas de seguridad diseñadas para garantizar que todas las empresas que acepten, procesen, almacenen o transmitan información de tarjetas de crédito mantengan un entorno seguro.
Soluciones de cumplimiento de VVD/VCF	VMware Validated Designs/VMware Cloud Foundation. VMware Validated Designs proporciona proyectos integrales exhaustivamente probados para crear y operar un centro de datos definido por software. Con las soluciones de conformidad de VVD/VCF, los clientes pueden cumplir con los requisitos de conformidad de varios reglamentos de la industria y del gobierno.

Referencia de controles de seguridad de vSphere

Las guías de fortalecimiento de seguridad de VMware proporcionan instrucciones prescriptivas para implementar y operar los productos de VMware de forma segura. Para vSphere, esta guía se denomina *Guía de configuración de seguridad de vSphere* (anteriormente conocida como *Guía de fortalecimiento*). A partir de vSphere 8.0 Update 3, la información de la *Guía de configuración de seguridad de vSphere* conocida como controles de seguridad, se incluye en esta guía.

Los controles de seguridad ofrecen prácticas recomendadas de seguridad para vSphere. Los controles de seguridad no corresponden directamente a directrices o marcos normativos. Por lo tanto, no los utilice como medio para lograr la conformidad. Además, los controles de seguridad no están diseñados para usarse como lista de comprobación de seguridad.

La seguridad siempre implica ceder en algo. Implementar controles de seguridad puede afectar negativamente la facilidad de uso, el rendimiento u otras tareas operativas. Tenga en cuenta las cargas de trabajo, los patrones de uso, la estructura organizativa, entre otros elementos, antes de realizar cambios de seguridad, ya sea que los consejos provengan de VMware o de otras fuentes del sector.

Si su organización tiene necesidades de conformidad normativa, consulte https://core.vmware.com/compliance. Este sitio incluye kits de conformidad y guías de auditoría de productos para ayudar a los administradores de vSphere y a los auditores normativos a garantizar y dar fe de la conformidad de la infraestructura virtual en cuanto a los marcos normativos, como NIST 800-53v4, NIST 800-171, PCI DSS, HIPAA, CJIS, ISO 27001, entre otros.

Estos controles de seguridad de vSphere no contemplan la protección de los siguientes elementos:

- Software que se ejecuta dentro de la máquina virtual, como el sistema operativo invitado y las aplicaciones
- Tráfico que se ejecuta a través de las redes de máquina virtual
- Seguridad de los productos de extensión

Estos controles de seguridad de vSphere no deben utilizarse como una herramienta de "cumplimiento". Estos controles de seguridad permiten dar los primeros pasos hacia el cumplimiento pero, por sí mismos, no garantizan que la implementación sea conforme. Para obtener más información sobre la conformidad, consulte Seguridad y conformidad en el entorno de vSphere.

No aplique ciegamente controles de seguridad a su entorno. En cambio, dedique un momento a evaluar cada ajuste y tome una decisión informada sobre si aplicarlo o no. Como mínimo, puede utilizar las instrucciones de las secciones de Evaluación para comprobar la seguridad de su implementación.

Estos controles de seguridad son una ayuda para comenzar a implementar la conformidad en su implementación. Cuando se utilizan con las guías de DISA y otras directrices de conformidad, puede establecer una correspondencia entre los controles de seguridad de vSphere y el tipo de conformidad de cada directriz.

Definiciones de los términos de los controles de seguridad

En las siguientes secciones de control de seguridad, se utilizan estos términos y definiciones.

Tabla 17-2. Definiciones de controles de seguridad

Término de los controles	Definición
Valor predeterminado de instalación	El valor predeterminado del control en esta versión de vSphere cuando instala el producto por primera vez.
Valor sugerido de línea base	Una recomendación razonable sobre cómo debe configurar este control, si no hay otras instrucciones presentes. Las instrucciones de cumplimiento normativo podrían sustituir a estas recomendaciones, por ejemplo.

Tabla 17-2. Definiciones de controles de seguridad (continuación)

Término de los controles	Definición
Acción necesaria	La acción sugerida para un control en particular. Modificar: realizar el cambio. Para los controles que están fuera de vSphere, como la configuración de hardware, esta documentación siempre asume que el control está establecido de forma no segura de forma predeterminada y recomienda modificar la configuración. Auditar: asegurarse de que el valor predeterminado esté en uso, que el valor esperado esté presente o que están documentadas las excepciones al control. Cuando se audita un control cuyo valor predeterminado es el valor sugerido, son posibles dos líneas de pensamiento. Primera: solo si se establecen los parámetros explícitamente se pueden auditar y conocer. Segunda: todos los cambios de configuración requieren "cuidado y mantenimiento" a lo largo del tiempo, así que cuando exista un valor predeterminado seguro, puede utilizarlo para ayudar a simplificar un entorno. Esta documentación sigue este último enfoque, pero puede elegir su propio criterio. Los controles no implementados no tienen ningún efecto sobre la seguridad. Se enumeran como "auditoría" en esta documentación, pero se pueden eliminar.
Impacto funcional potencial si se cambia el valor predeterminado	¿Este cambio puede causar problemas? La mayoría de los controles de seguridad presentan compromisos de algún tipo. ¿Qué exigiría a cambio la modificación de este control?
Evaluación mediante comandos de PowerCLI	Un ejemplo de comando PowerCLI para determinar cómo se establece el control.
Ejemplo de corrección mediante un comando de PowerCLI	Un ejemplo de comando PowerCLI para establecer el control según la recomendación.

Referencia de controles de seguridad para diseño del sistema de vSphere

Estos controles de seguridad proporcionan un conjunto de líneas base de prácticas recomendadas de diseño del sistema de vSphere.

Eliminar de vCenter Server complementos de terceros

Reduzca o elimine los complementos de vCenter Server de terceros.

La instalación de complementos y otras interconexiones de terceros entre sistemas puede erosionar las delimitaciones entre diferentes sistemas de infraestructura, lo que ofrece oportunidades para los atacantes que han comprometido un sistema para desplazarse lateralmente a otro. La combinación estrecha de otros sistemas con vSphere a menudo también

crea impedimentos para aplicar parches y actualizaciones a tiempo. Asegúrese de que todo complemento (de terceros o no) para los componentes de vSphere aporte utilidad. Si decide utilizar complementos en lugar de consolas de administración individuales, asegúrese de que su uso compense los riesgos que crean.

Precaución con las interfaces de administración de infraestructuras

Tenga cuidado al conectar interfaces de administración de infraestructuras a orígenes de autorización y autenticación de propósito general.

Los directorios empresariales centralizados son el destino de los atacantes debido a su función en la autorización en toda una empresa. Un atacante puede moverse libremente dentro de una organización una vez que ese directorio esté comprometido. La conexión de la infraestructura de TI a directorios centralizados ha demostrado ser un riesgo considerable para el ransomware y otros ataques. Aísle la autenticación y la autorización de todos los sistemas de infraestructura.

Para ESXi:

- Realice toda la administración de hosts a través de vCenter Server
- Desactivar ESXi Shell
- Ponga ESXi en modo de bloqueo normal
- Establezca como contraseña raíz de ESXi una contraseña compleja

Active vSphere Distributed Resource Scheduler

Active vSphere Distributed Resource Scheduler (DRS) en el modo Totalmente automatizado.

vSphere DRS utiliza vMotion para mover cargas de trabajo entre hosts físicos a fin de garantizar el rendimiento y la disponibilidad. El modo totalmente automatizado garantiza que el vSphere Lifecycle Manager pueda funcionar con DRS para activar las operaciones de aplicación de revisiones y actualizaciones.

Si se necesitan asignaciones de máquina virtual a host específicas, utilice reglas DRS. Siempre que sea posible, utilice reglas "should" en lugar de "must" para poder suspender la regla temporalmente durante la aplicación de revisiones y la recuperación de alta disponibilidad.

Active vSphere High Availability

vSphere High Availability (HA) reinicia las cargas de trabajo en otros hosts ESXi de un clúster si se produce un error repentino en un host ESXi. Asegúrese de que la configuración de HA esté configurada correctamente para su entorno.

Active Enhanced vMotion Compatibility

vSphere Enhanced vMotion Compatibility (EVC) garantiza que las cargas de trabajo se puedan migrar en vivo mediante vMotion entre hosts ESXi de un clúster que usan diferentes generaciones de CPU. EVC también ayuda en situaciones con vulnerabilidades de CPU, donde es posible que se introduzcan nuevas instrucciones de microcódigo en las CPU, lo que las hace temporalmente incompatibles entre sí.

Proteja los sistemas contra alteraciones

Asegúrese de que los hosts ESXi y los componentes de redes y almacenamiento relacionados estén protegidos contra alteraciones, accesos no autorizados y eliminación no autorizada. Además, proteja los hosts de los daños causados por factores ambientales como las inundaciones, las temperaturas extremas (bajas o altas) y el polvo y los desechos.

El uso de características de seguridad, como vSphere Native Key Provider y la persistencia de claves de ESXi, podría provocar que el material seguro se almacene localmente en hosts ESXi, lo que permite que los atacantes arrancar y desbloquear clústeres que deberían estar protegidos. Es importante tener en cuenta la seguridad física y las amenazas reales, como el robo.

Más allá del robo, tener en cuenta la seguridad también significa hacerse preguntas a sí mismo y a la organización como las siguientes:

- ¿Qué podría ir mal?
- ¿Cómo sabría si algo fue mal?

Estas preguntas adquieren una mayor importancia cuando se trata de ubicaciones de centros de datos sin personal y de instalaciones de colocación. Con respecto a los centros de datos y las configuraciones de rack, hágase las siguientes preguntas:

- ¿Las puertas del centro de datos se cierran automáticamente y se bloquean correctamente por sí solas?
- Si se dejaran las puertas entreabiertas, ¿se generaría una alerta proactiva?
- Si las puertas del rack están bloqueadas, ¿sería posible acceder al rack desde un lateral o la parte superior y desconectar un cable? ¿Puede una persona no autorizada conectar un cable a un conmutador de red?
- ¿Es posible quitar un dispositivo, como un dispositivo de almacenamiento o incluso un servidor completo? ¿Qué sucedería en tal caso?

Otras preguntas que se podría hacer incluyen:

- ¿Podría alguien recoger información sobre su entorno o su empresa a partir de pantallas de información en los servidores, como paneles LCD o consolas?
- Si esas pantallas de información están inactivas, ¿podrían activarse desde fuera del rack, por ejemplo, con el uso de un cable rígido?
- ¿Hay otros botones, como el botón de encendido, que se podrían pulsar para crear una interrupción del servicio en su empresa?

Por último, pregúntese, ¿hay otras amenazas físicas, como la posibilidad de inundaciones, congelación, calor elevado o polvo y desechos del medio ambiente, que afectarían a la disponibilidad?

Asigne nombre a los objetos de vSphere de forma descriptiva

Asegúrese de asignar nombre a los objetos de vSphere de forma descriptiva, cambiando los nombres predeterminados de los objetos para garantizar la precisión y reducir posibles confusiones.

Utilice prácticas recomendadas de nomenclatura para los objetos de vSphere, cambiando los nombres predeterminados, como "Centro de datos", "Almacén de datos de vSAN", "DSwitch", "Red de máquina virtual", etc., para incluir información adicional. Esto ayuda a mejorar la precisión y reducir los errores al desarrollar, implementar y auditar políticas de seguridad y procesos operativos.

Los grupos de puertos que utilizan el etiquetado de VLAN 802.1Q pueden incluir el número de VLAN. Los nombres de centros de datos y clústeres pueden reflejar ubicaciones y propósitos. Los nombres de almacenes de datos y conmutadores distribuidos virtuales podrían reflejar los nombres de los centros de datos y los clústeres a los que están conectados. Los nombres de proveedores de claves son particularmente importantes, especialmente cuando se protegen máquinas virtuales cifradas con replicación en sitios alternativos. Trabaje para evitar posibles "colisiones de nombres" con objetos presentes en otros centros de datos y clústeres.

Algunas organizaciones no asignan nombres a sistemas con identificadores de ubicación física, como direcciones postales, y prefieren ocultar la ubicación física de los centros de datos mediante el uso de términos como "Sitio A", "Sitio B", etc. Esto también ayuda si los sitios se reubican, lo que evita la necesidad de cambiar el nombre de todo o mantener información imprecisa.

Al decidir un esquema de nomenclatura, tenga en cuenta que muchos objetos pueden tener propiedades similares. Por ejemplo, dos grupos de puertos pueden tener la misma VLAN asignada, pero tienen reglas de filtrado y marcado de tráfico diferentes. Puede resultar útil incorporar un nombre de proyecto o una descripción breve en el nombre para diferenciar los objetos de este tipo.

Por último, considere la automatización al desarrollar un esquema de nomenclatura. Los nombres que se pueden derivar mediante programación suelen ser útiles para crear scripts y automatizar tareas.

Aislar interfaces de administración de infraestructura

Asegúrese de que las interfaces de administración de la infraestructura de TI estén aisladas en su propio segmento de red o como parte de una red de administración aislada.

Asegúrese de que todas las interfaces de administración configuradas para los componentes de virtualización estén en un segmento de red (VLAN, etc.) dedicado solo a la administración de virtualización, sin cargas de trabajo ni sistemas no relacionados. Asegúrese de que las interfaces de administración se controlen con controles de seguridad del perímetro, de modo que solo los administradores de vSphere autorizados puedan acceder a esas interfaces desde estaciones de trabajo autorizadas.

Algunos diseños de sistemas colocan vCenter Server y otras herramientas de administración en sus propios segmentos de red, aislados de ESXi, ya que así consiguen una mejor supervisión de esos sistemas. Otros diseños ponen vCenter Server con la administración de ESXi debido a la relación entre estos dos productos y la posibilidad de errores de configuración del firewall o interrupciones que interrumpan el servicio. Sea cual sea el diseño que elija, hágalo con cuidado.

Usar vMotion correctamente

Asegúrese de que vMotion utilice cifrado de datos en tránsito (establecido en "Requerido" para las máquinas virtuales). Y asegúrese de que las interfaces de red de VMkernel utilizadas para vMotion estén aisladas en sus propios segmentos de red que tengan controles perimetrales.

vMotion y Storage vMotion copian la memoria y los datos de almacenamiento de las máquinas virtuales, respectivamente, por toda la red. Asegurarse de que los datos estén cifrados en tránsito garantiza la confidencialidad. El aislamiento en un segmento de red dedicado con los controles de perímetro adecuados puede añadir defensa en profundidad y también permitir la gestión del tráfico de red.

Al igual que todas las formas de cifrado, el cifrado de vMotion introduce una pérdida de rendimiento, pero ese cambio de rendimiento se produce en el proceso de vMotion en segundo plano y no afecta al funcionamiento de la máquina virtual.

Use vSAN correctamente

Asegúrese de que vSAN utilice cifrado de datos en tránsito y asegúrese de que las interfaces de red de VMkernel utilizadas para vSAN estén aisladas en sus propios segmentos de red que tengan controles de perímetro.

vSAN incluye cifrado de datos en tránsito que puede ayudar a mantener la confidencialidad cuando los nodos de vSAN se comunican. Al igual que ocurre con muchos controles de seguridad, existe un compromiso con el rendimiento. Supervise el rendimiento y la latencia de almacenamiento a medida que se activa el cifrado de datos en tránsito. Las organizaciones que no activan o no pueden activar el cifrado de datos en tránsito de vSAN deben aislar el tráfico de red en un segmento de red dedicado con los controles perimetrales adecuados.

Activar Network I/O Control

Para asegurarse de tener resistencia a la denegación de servicio de red, active Network I/O Control (NIOC).

Network I/O Control (NIOC) de vSphere es una tecnología de administración de tráfico que ofrece calidad de servicio en el nivel del hipervisor, lo que mejora el rendimiento de la red mediante la priorización de recursos en entornos de carga de trabajo compartidos y de nube de varios tenants. Incorporado en el vSphere Distributed Switch (vDS), NIOC particiona el ancho de banda del adaptador de red en "grupos de recursos de red" que corresponden a diferentes tipos de tráfico, como el tráfico de administración y vMotion. El uso de NIOC permite a los usuarios asignar recursos compartidos, límites y reservas a estos grupos.

NIOC conserva la disponibilidad de red para los servicios esenciales y evita la congestión al limitar el tráfico menos crítico. Esto se logra habilitando la creación de directivas de control de red según los requisitos empresariales, garantizando el aislamiento de los tipos de tráfico y permitiendo la reasignación de recursos dinámicos en función de la prioridad y el uso.

No configurar VLAN reservadas por el proveedor

Asegúrese de que los vínculos superiores del conmutador físico de los hosts ESXi no estén configurados con VLAN reservadas por el proveedor.

Algunos proveedores de red reservan identificadores de VLAN particular es para uso interno o específico. Asegúrese de que las configuraciones de red de vSphere no incluyan estos valores.

Configurar vínculos superiores de ESXi como puertos de acceso

Asegúrese de que los vínculos superiores de conmutadores físicos de hosts ESXi estén configurados como "puertos de acceso" asignados a una sola VLAN o como enlaces troncales de VLAN 802.1Q etiquetados sin VLAN nativa. Asegúrese de que los grupos de puertos de vSphere no permitan el acceso a VLAN 1 o VLAN nativas sin etiquetar.

Las conexiones de red que tienen una VLAN "nativa" configurada para aceptar tráfico sin etiquetas o que tienen acceso a VLAN 1 pueden ofrecer oportunidades para que los atacantes diseñen paquetes especializados que burlan los controles de seguridad de la red. VLAN 1 es la red predeterminada que se suele utilizar para la administración de redes y las comunicaciones y debe aislarse de las cargas de trabajo. Asegúrese de que los grupos de puertos no estén configurados para acceder a las VLAN nativas. Asegúrese de que los puertos troncales de VLAN estén configurados con definiciones específicas de VLAN (no con "all"). Por último, asegúrese de que los grupos de puertos estén configurados correctamente para que los atacantes no puedan utilizar un entorno virtualizado para eludir los controles de seguridad de red.

Configurar conexiones de tejido de almacenamiento correctamente

Asegúrese de que las conexiones del tejido de almacenamiento utilicen cifrado de datos en tránsito o estén aisladas en sus propios segmentos de red o SAN que tengan controles perimetrales.

La protección de los datos de almacenamiento durante el tránsito ayuda a garantizar la confidencialidad de los datos. El cifrado no es una opción para muchas tecnologías de almacenamiento, a menudo debido a problemas de disponibilidad o rendimiento. En esos casos, el aislamiento en un segmento de red dedicado con los controles perimetrales adecuados puede ser un control compensador eficaz y puede agregar una defensa en profundidad.

Usar enmascaramiento de LUN en sistemas de almacenamiento

Asegúrese de que los sistemas de almacenamiento utilicen enmascaramiento de LUN, zonificación y otras técnicas de seguridad del lado del almacenamiento para garantizar que las asignaciones de almacenamiento solo sean visibles para el clúster de vSphere en el que se utilizará.

El enmascaramiento de LUN en la controladora de almacenamiento y la división en zonas de SAN ayudan a garantizar que el tráfico de almacenamiento no sea visible para hosts no autorizados y que estos no puedan montar almacenes de datos, omitiendo otros controles de seguridad.

Limitar conexiones a los sistemas autorizados

Considere el uso del firewall de vCenter Server Appliance para limitar las conexiones a los sistemas y administradores autorizados.

vCenter Server Appliance contiene un firewall básico que puede utilizar para limitar las conexiones entrantes a vCenter Server. Esta puede ser una capa eficaz de defensa en profundidad junto con los controles de seguridad del perímetro.

Como siempre, antes de agregar reglas para bloquear conexiones, asegúrese de que haya reglas implementadas para permitir el acceso desde las estaciones de trabajo administrativas.

No almacenar claves de cifrado en hosts ESXi sin proteger el acceso físico

El entorno no debe almacenar claves de cifrado en hosts ESXi sin proteger también el acceso físico a los hosts.

Para evitar bucles de dependencia, vSphere Native Key Provider almacena las claves de descifrado directamente en los hosts ESXi, ya sea en un módulo de plataforma de confianza (Trusted Platform Module, TPM) o como parte de la configuración de ESXi cifrada. Sin embargo, si no protege físicamente un host y un atacante roba el host, el atacante posee los medios para desbloquear y ejecutar cargas de trabajo cifradas. Por lo tanto, es fundamental garantizar la seguridad física (consulte Proteja los sistemas contra alteraciones) u optar por utilizar un proveedor de claves estándar (consulte Qué es un proveedor de claves estándar) que incluya controles de seguridad de red adicionales.

Utilizar dispositivos persistentes, no SD y no USB de tamaño adecuado para volúmenes de arranque ESXi

El entorno debe utilizar dispositivos persistentes, no SD y no USB de tamaño adecuado para los volúmenes de arranque ESXi.

La memoria flash es un componente que se desgasta con el tiempo y cada escritura de datos acorta su duración. Los SSD y los dispositivos NVMe tienen características integradas para reducir este desgaste, lo que hace que sean más fiables. Sin embargo, las tarjetas SD y la mayoría de unidades flash USB no tienen estas características y pueden desarrollar problemas de fiabilidad, como sectores defectuosos, a menudo sin signos evidentes.

Para reducir el desgaste y hacer que los dispositivos SD y USB duren más tiempo, cuando instale ESXi en estos dispositivos, puede guardar los registros de auditoría y del sistema en un disco RAM en lugar de escribir constantemente en el dispositivo. Esto significa que debe configurar nuevas ubicaciones de almacenamiento a largo plazo para estos registros y cambiar la salida de los registros para que vaya a esas nuevas ubicaciones.

Elegir un dispositivo de arranque fiable elimina estos pasos adicionales y ayuda a ESXi a pasar automáticamente auditorías de seguridad.

Configurar correctamente el destino iSCSI de vSAN

Asegúrese de que el destino iSCSI de vSAN utilice sus propias interfaces de red de VMkernel, aisladas en su propio segmento de red y empleando controles perimetrales separados mediante el filtrado y marcado de tráfico del grupo de puertos distribuidos, NSX o controles de seguridad de red externos.

Debido a que los clientes del destino iSCSI son externos al clúster, aíslelos en sus propias interfaces de red. De esta manera, puede restringir por separado otras comunicaciones de red solo internas. El aislamiento de este tipo también ayuda a diagnosticar y administrar el rendimiento.

Referencia de controles de seguridad de hardware de vSphere

Estos controles de seguridad proporcionan un conjunto de líneas base de prácticas recomendadas de seguridad para el hardware de vSphere. Están estructurados de manera tal que se explican los beneficios y las compensaciones de la implementación del control.

Variable utilizada

Los comandos de PowerCLI de esta sección utilizan la siguiente variable:

- $ESXi = "*host_name*"

Usar tecnología de ejecución de confianza de Intel

Asegúrese de que Intel Trusted Execution Technology (TXT) esté activada, si está disponible en el firmware del sistema.

Las plataformas Intel Xeon Scalable Processor tienen TXT, que proporciona la autenticidad de una plataforma y su sistema operativo. Cuando se activa, ESXi aprovecha las ventajas de seguridad que ofrece esta tecnología.

Valor sugerido

Activado

Impacto potencial si se cambia el valor predeterminado

En ocasiones, las implementaciones tempranas de TXT provocaban apagados repentinos del sistema, activación de alarmas de atestación en vCenter Server o incluso errores de arranque. El reinicio del sistema resuelve estos problemas, mientras que la actualización del firmware del sistema, por lo general, los resuelve de forma permanente. Consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/78243.

Evaluación mediante comandos de PowerCLI

```
(Get-VMHost -Name $ESXi | Get-View).Capability.TxtEnabled
```

Configurar el arranque seguro UEFI

Asegúrese de que el arranque seguro UEFI esté activado.

La activación del arranque seguro UEFI en el hardware de un host ESXi ayuda a evitar malware y configuraciones que no son de confianza.

Valor sugerido

Activado

Impacto potencial si se cambia el valor predeterminado

La activación del arranque seguro UEFI después de la instalación podría evitar que se inicie un host ESXi. Ejecute `/usr/lib/vmware/secureboot/bin/secureBoot.py -c` en un host de ejemplo para determinar si puede activar el arranque seguro de forma segura.

Evaluación mediante comandos de PowerCLI

N/C

Usar TPM 2.0

Asegúrese que hay un módulo de plataforma de confianza (Trusted Platform Module, TPM) 2.0 instalado y configurado correctamente en los hosts ESXi.

ESXi pueden utilizar un TPM para activar funciones de seguridad avanzadas que evitan el malware, eliminan dependencias y protegen las operaciones del ciclo de vida del hardware. Cuando sea posible, configure los hosts para que usen TPM 2.0 y active el TPM en el firmware del sistema.

Valor sugerido

TPM 2.0 instalado y activado (hash SHA-256, interfaz TIS/FIFO)

Impacto potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
(Get-VMHost -Name $ESXi | Get-View).Capability.TpmSupported
(Get-VMHost -Name $ESXi | Get-View).Capability.TpmVersion
```

Asegúrese de que el firmware del hardware esté actualizado

Asegúrese de aplicar las actualizaciones de firmware más recientes a todos los componentes de los sistemas y de que el firmware sea auténtico y lo suministre el fabricante del hardware.

El firmware del hardware no es inmune a problemas graves que afectan a la confidencialidad, la integridad o la disponibilidad. Los atacantes pueden utilizar controladores de administración del sistema y motores de administración vulnerables para establecer persistencia y volver a infectar y poner en peligro los hosts después de los reinicios y las actualizaciones.

Valor sugerido

N/C

Impacto potencial si se cambia el valor predeterminado

Si utiliza vSAN, asegúrese de que el dispositivo de almacenamiento y las versiones de firmware de la controladora estén certificados.

Evaluación mediante comandos de PowerCLI

N/C

Controladoras de administración de hardware integradas y seguras

Asegúrese de que las controladoras de administración de hardware integradas estén totalmente protegidas.

Muchos servidores tienen controladoras de administración de hardware integradas que pueden ser sumamente útiles para supervisar y actualizar hardware, configuración y firmware. Para estas controladoras:

- Desactive todas las funcionalidades no utilizadas.
- Deshabilite todos los métodos de acceso no utilizados.
- Establezca contraseñas y controles de contraseñas.
- Establezca firewalls y control de acceso para que el acceso solo se produzca desde estaciones de trabajo con acceso autorizado para el equipo de administración de virtualización.

Desactive todas las opciones de configuración de "primer arranque", especialmente aquellas que vuelvan a configurar el sistema desde un dispositivo USB insertado. Además, desactive o proteja los puertos USB conectados a controladoras de administración. Siempre que sea posible, configure los puertos USB para que solo admitan teclados.

Cambie las contraseñas predeterminadas de las cuentas.

Proteja las pantallas de información externas para evitar que se filtre información. Proteja los botones de encendido y de información contra el uso no autorizado.

Muchos controladores de administración de hardware proporcionan mecanismos de alerta cuando se producen errores de hardware y cambios de configuración. Considere la posibilidad de utilizarlos si no utiliza otro método para la supervisión del hardware.

Valor sugerido

N/C

Impacto potencial si se cambia el valor predeterminado

La desactivación de los métodos de conexión podría provocar futuros cambios de supervisión y administración en las configuraciones de la controladora de administración de hardware en los servidores implementados. Siempre que sea posible, utilice métodos de administración de CLI y API que pueda implementar usando scripts en lugar de utilizar

aplicaciones o software de administración adicionales. Aprender estas técnicas ahorra tiempo, evita el esfuerzo adicional de instalar y mantener herramientas adicionales y permite realizar cambios de configuración a tiempo.

Evaluación mediante comandos de PowerCLI

N/C

Sincronizar la hora de las controladoras de administración de hardware integradas

Asegúrese de sincronizar la hora de las controladoras de administración de hardware integradas.

La criptografía, el registro de auditoría, las operaciones del clúster y las respuestas a incidentes dependen de la hora sincronizada. Esta recomendación se extiende a todos los dispositivos de la infraestructura. El protocolo de tiempo de red (NTP) debe tener al menos cuatro orígenes. Si debe elegir entre dos orígenes y un origen, es preferible uno solo.

Valor sugerido

Específico del sitio o:

0.vmware.pool.ntp.org,

1.vmware.pool.ntp.org,

2.vmware.pool.ntp.org,

3.vmware.pool.ntp.org

Impacto potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

N/C

Proteger la forma en que las controladoras de administración de hardware integradas usan Active Directory

Asegúrese de no crear un bucle de dependencia o un vector de ataque por la forma en que las controladoras de administración de hardware integradas utilizan Active Directory.

Desactive las conexiones con Active Directory, o como mínimo, considérelas como vectores de ataque y bucles de dependencia (para autenticación, autorización, DNS, DHCP y hora). Considere la posibilidad de administrar cuentas locales en estos dispositivos a través de API y CLI. Si debe utilizar Active Directory para la autenticación, utilice la autorización local para que los atacantes con acceso a Active Directory no puedan promocionarse a sí mismos mediante la pertenencia a grupos.

Valor sugerido

N/C

Impacto potencial si se cambia el valor predeterminado

No conectar controladoras de administración de hardware a fuentes de autorización y autenticación centralizadas implica una administración adicional. La mayoría de los controladores de administración de hardware tienen kits de herramientas de CLI o API para automatizar el proceso.

Evaluación mediante comandos de PowerCLI

N/C

Desactivar controladoras de administración de hardware integradas virtuales

Asegúrese de que estén desactivadas las controladoras de administración de hardware integradas con interfaces de red internas, emuladas o virtuales.

Algunas controladoras de administración de hardware tienen la capacidad de presentar interfaces de red virtual para ESXi como una interfaz de administración. Estos enfoques crean posibles puertas traseras de acceso que los atacantes pueden utilizar para burlar los cortafuegos perimetrales y basados en red, en cualquier dirección, y para evitar ser observados por IDS, IPS y herramientas de análisis de amenazas. En muchos casos, esta funcionalidad no es estrictamente necesaria para administrar hosts.

Valor sugerido

N/C

Impacto potencial si se cambia el valor predeterminado

La desactivación de redes internas puede limitar la eficacia de la herramienta de administración de proveedores.

Evaluación mediante comandos de PowerCLI

N/C

Activar SEV-ES de AMD

Asegúrese de activar Secure Encrypted Virtualization-Encrypted State (SEV-ES) de AMD, si está disponible en el firmware del sistema. Asegúrese de que el valor mínimo de ASID de elementos SEV y sin estado cifrado sea igual al número de máquinas virtuales SEV-ES más una.

Las plataformas AMD EPYC admiten SEV-ES, una tecnología para cifrar el estado de registro de cpu y memoria, y limitar la visibilidad para el hipervisor, con el fin de aumentar la seguridad de la carga de trabajo y reducir la exposición a ciertos tipos de ataques. Cuando se configura correctamente, SEV-ES proporciona seguridad mejorada al sistema operativo invitado en máquinas virtuales y contenedores en vSphere y vSphere with Tanzu. La activación de SEV-ES en el firmware del sistema facilita la habilitación futura dentro de las máquinas virtuales, los contenedores y los sistemas operativos invitados.

Valor sugerido

Activado (el ASID mínimo de elementos SEV no-ES es igual al número de máquinas virtuales SEV-ES más una)

Impacto potencial si se cambia el valor predeterminado

El sistema operativo invitado de una máquina virtual debe ser compatible con SEV-ES y, por lo tanto, limita algunas características, como vMotion, instantáneas, etc. Para obtener más información sobre estas alternativas, consulte Funciones de VMware no admitidas en SEV-ES.

Evaluación mediante comandos de PowerCLI

N/C

Activar Virtual Intel Software Guard Extensions (vSGX)

Asegúrese de que Virtual Intel® Software Guard Extensions (vSGX) esté activado, si está disponible en el firmware del sistema.

Las plataformas de procesador escalable Intel Xeon tienen Software Guard Extensions, o SGX, una tecnología que ayuda a las aplicaciones a proteger los datos en la memoria del sistema. Cuando se configura correctamente, vSphere admite el uso de SGX dentro de las máquinas virtuales. Habilitar SGX en el firmware del sistema facilita la habilitación futura dentro de las máquinas virtuales y los sistemas operativos invitados.

Valor sugerido

Sugerido: Activado (software, desbloqueado)

Impacto potencial si se cambia el valor predeterminado

El sistema operativo invitado de una máquina virtual debe admitir vSGX y, por lo tanto, limita algunas características, como vMotion, instantáneas, etc. Para obtener más información sobre estas alternativas, consulte Funciones de VMware no admitidas en vSGX.

Evaluación mediante comandos de PowerCLI

```
(Get-VMHost -Name $ESXi | Get-View).Capability.SgxRegistrationSupported
```

Desactivar puertos externos

Asegúrese de que los puertos externos sin utilizar estén desactivados o protegidos contra el uso no autorizado.

Los atacantes pueden utilizar puertos no utilizados, especialmente USB, para conectar teclados, redes y almacenamiento. Tome medidas razonables para controlar el acceso a estos puertos, como deshabilitarlos y controlar el acceso. Siempre que sea posible, utilice otros medios, como puertas de rack, paneles laterales de rack y pisos resistentes que no permitan acceder a los puertos desde fuera del rack cuando la puerta del rack esté cerrada. Tenga en cuenta que los cables caben fácilmente a través de muchos huecos dentro y alrededor de los bastidores y puertas de rack, y se pueden utilizar hilos rígidos para meter cables en las tomas desde fuera del rack, así como para desprender cables para crear una interrupción del servicio.

Siempre que sea posible, configure los puertos USB para que solo admitan teclados.

Al desactivar este tipo de funcionalidad, tenga en cuenta que es posible que necesite acceder a un servidor con un teclado USB durante una interrupción o como parte de las operaciones de ciclo de vida, y planifique según corresponda.

Valor sugerido

N/C

Impacto potencial si se cambia el valor predeterminado

La seguridad siempre implica ceder en algo. Cuando considere un control de seguridad, como la desactivación de puertos externos, incluya en la ecuación la facilidad de recuperación tras una interrupción o un incidente. En este caso, la desactivación de los puertos externos afecta a la capacidad de utilizar la consola de ESXi en caso de emergencia.

Algunos servidores pueden desactivar y activar de forma dinámica ciertos puertos USB para la administración. Asegúrese de que la elección de este control de seguridad cumpla con las necesidades de su organización y pruebe siempre esos métodos antes de implementarlos.

Evaluación mediante comandos de PowerCLI

N/C

Referencia de controles de seguridad de ESXi

Estos controles de seguridad proporcionan un conjunto de líneas base de prácticas recomendadas de seguridad de ESXi. Están estructurados de manera tal que se explican los beneficios y las compensaciones de la implementación del control. La mayoría de los controles están en forma de configuración avanzada del sistema. Para cambiar la configuración avanzada del sistema, puede utilizar la instancia de PowerCLI proporcionada o vSphere Client (**Host > Configurar > Sistema > Configuración avanzada del sistema**).

Variable utilizada

Los comandos de PowerCLI de esta sección utilizan las siguientes variables:

- $ESXi = "*host_name*"
- $vmkernel_interface = "*vmkernel_adapter*"

Garantizar que se deniegue el acceso a la cuenta de DCUI

El host ESXi debe denegar el acceso al shell de la cuenta de usuario dcui.

La cuenta de usuario dcui se utiliza para el aislamiento de procesos de la propia DCUI. Para reducir la superficie de ataque, desactive el acceso al shell de la cuenta de usuario dcui.

Valores

Valor predeterminado de instalación: True

Valor sugerido de línea base: False

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.account.list.Invoke() | Where-Object { $_.UserID -eq 'dcui' } | Select-
Object -ExpandProperty Shellaccess
```

Ejemplo de corrección mediante un comando de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.system.account.set.CreateArgs()
$arguments.id = "dcui"
$arguments.shellaccess = "false"
$ESXcli.system.account.set.Invoke($arguments)
```

Annotations.WelcomeMessage

Configura el texto del mensaje de inicio de sesión que se muestra en VMware Host Client y la DCUI.

ESXi permite mostrar un mensaje de inicio de sesión. Los usos del mensaje de inicio de sesión incluyen informar a los intrusos que sus actividades son ilegales, y transmitir a los usuarios autorizados las expectativas y las obligaciones que deben cumplir y aceptar al utilizar el sistema.

Valores

Valor predeterminado de instalación: no definido

Valor sugerido de línea base: consulte a los asesores legales de su organización para obtener el texto que se aplica a su entorno.

Texto del mensaje de ejemplo: solo usuarios autorizados. El uso real o el intento de uso no autorizados de este sistema está prohibido y puede dar lugar a procedimientos o sanciones penales, civiles, de seguridad o administrativos. El uso de este sistema de información indica el consentimiento para la supervisión y el registro, sin previo aviso o permiso. Los usuarios no tienen expectativas de privacidad cuando usan este sistema. Cualquier información almacenada en este sistema, o en tránsito, u obtenida mediante la supervisión o registro, puede divulgarse a las autoridades policiales o utilizarse de acuerdo con la legislación federal, los estatutos estatales y la directiva de la organización. Si no es un usuario autorizado de este sistema, salga de él en este momento.

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Enmascara la información de "F2/F12" y la dirección IP en la DCUI. También puede requerir documentación y formación de su entorno.

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Annotations.WelcomeMessage
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Annotations.WelcomeMessage | Set-
AdvancedSetting -Value "your_message"
```

Config.HostAgent.vmacore.soap.sessionTimeout

Configura un tiempo de espera de sesión para vSphere API.

Esta práctica mitiga los posibles riesgos de seguridad al garantizar que las sesiones sin supervisión, que los usuarios no autorizados o el software malicioso podrían aprovechar, no se dejen abiertas de forma indefinida.

Valores

Valor predeterminado de instalación: 30

Valor sugerido de línea base: 30

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Config.HostAgent.vmacore.soap.sessionTimeout
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Config.HostAgent.vmacore.soap.sessionTimeout
| Set-AdvancedSetting -Value 30
```

Config.Etc.issue

Configura el texto del aviso cuando un usuario se conecta a un host ESXi mediante SSH.

ESXi proporciona la capacidad de mostrar un aviso para las conexiones de SSH. Los usos del aviso incluyen informar a los intrusos de que sus actividades son ilegales, y transmitir a los usuarios autorizados las expectativas y obligaciones que deben cumplir y aceptar al utilizar el sistema. Mantenga el servicio de SSH desactivado, a menos que esté realizando operaciones de solución de problemas. Una incoherencia de implementación entre ESXi y vCenter Server requiere que el "problema" en `Config.Etc.issue` esté en minúsculas para funcionar en ambos escenarios.

Valores

Valor predeterminado de instalación: no definido

Valor sugerido de línea base: consulte a los asesores legales de su organización para obtener el texto que se aplica a su entorno.

Texto del mensaje de ejemplo: solo usuarios autorizados. El uso real o el intento de uso no autorizados de este sistema está prohibido y puede dar lugar a procedimientos o sanciones penales, civiles, de seguridad o administrativos. El uso de este sistema de información indica el consentimiento para la supervisión y el registro, sin previo aviso o permiso. Los usuarios no tienen expectativas de privacidad cuando usan este sistema. Cualquier información almacenada en este sistema, o en tránsito, u obtenida mediante la supervisión o registro, puede divulgarse a las autoridades policiales o utilizarse de acuerdo con la legislación federal, los estatutos estatales y la directiva de la organización. Si no es un usuario autorizado de este sistema, salga de él en este momento.

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Config.Etc.issue
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Config.Etc.issue | Set-AdvancedSetting
-Value "****************************************************************************`n*
Authorized users only. Actual or attempted unauthorized use of this      *`n* system
is prohibited and may result in criminal, civil, security, or     *`n* administrative
proceedings and/or penalties. Use of this information     *`n* system indicates consent to
monitoring and recording, without notice     *`n* or permission. Users have no expectation
of privacy. Any information     *`n* stored on or transiting this system, or obtained
by monitoring and/or    *`n* recording, may be disclosed to law enforcement and/or used
in accordance *`n* with Federal law, State statute, and organization policy. If you
are not *`n* an authorized user of this system, exit the system at this time.
*`n****************************************************************************`n"
```

Desactivar el acceso al shell para vpxuser

El host ESXi debe denegar el acceso al shell de la cuenta vpxuser.

vCenter Server crea la cuenta vpxuser cuando se asocia por primera vez un host ESXi. Posteriormente, la cuenta vpxuser se utiliza para la autenticación con privilegios para ESXi. Mientras que vCenter Server rota automáticamente la contraseña de la cuenta vpxuser en un intervalo regido por la opción `VirtualCenter.VimPasswordExpirationInDays`, la cuenta vpxuser también tiene acceso al shell. Desactive la cuenta vpxuser para reducir la superficie de ataque.

Valores

Valor predeterminado de instalación: True

Valor sugerido de línea base: False

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Las cuentas de usuario que no tienen acceso al shell no pueden reconfigurar el acceso al shell de otros usuarios, independientemente de sus niveles de privilegio. Debido a que vCenter Server se conecta a un host ESXi como la cuenta vpxuser, una vez que desactive el acceso al shell para vpxuser, ya no se podrá utilizar para cambiar esa configuración de cuenta para otras cuentas. Debe producirse una reconfiguración adicional host por host mediante el uso de una cuenta que esté autorizada.

ESXi 8.0 y versiones posteriores ya no admiten operaciones tradicionales de recuperación de cuentas o contraseñas, como el arranque desde medios o el cambio de init a un shell durante el arranque.

Asegúrese de que el host ESXi conserve al menos una cuenta de usuario con todos los privilegios y de proteger esta cuenta según corresponda.

Evaluación mediante comandos de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.account.list.Invoke() | Where-Object { $_.UserID -eq 'vpxuser' } | Select-Object -ExpandProperty Shellaccess
```

Ejemplo de corrección mediante un comando de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.system.account.set.CreateArgs()
$arguments.id = "vpxuser"
$arguments.shellaccess = "false"
$ESXcli.system.account.set.Invoke($arguments)
```

vCenter Server debe utilizar vSphere Authentication Proxy para evitar el almacenamiento de credenciales de Active Directory

vSphere Authentication Proxy permite que vCenter Server se conecte a entidades de Active Directory y las administre sin necesidad de almacenar directamente las credenciales de Active Directory, lo que reduce el riesgo de exposición o uso indebido de las credenciales.

Valores

Valor predeterminado de la instalación: no configurado

Valor sugerido de línea base: configúrelo si utiliza la función

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Get-VMHostAuthentication | Select-Object VMHost,Domain,DomainMembershipStatus
```

Ejemplo de corrección mediante un comando de PowerCLI

N/C

DCUI.Access

El host ESXi debe tener una lista DCUI.Access precisa.

Establece la lista de usuarios con excepción en modo de bloqueo para que contenga una lista precisa de usuarios y garantiza que solo los usuarios autorizados tengan acceso directo a la interfaz de usuario de la consola (DCUI) al host ESXi cuando se active el modo de bloqueo.

No puede eliminar el usuario raíz de la lista.

Para controlar el acceso a ESXi Shell y a SSH, utilice la lista de usuarios con excepción en modo de bloqueo. Consulte Garantizar que el host ESXi tenga una lista precisa de usuarios con excepción.

Valores

Valor predeterminado de instalación: raíz

Valor sugerido de línea base: raíz

Acción necesaria

Realice una auditoría de la lista.

Impacto funcional potencial si se cambia el valor predeterminado

Posible pérdida de acceso administrativo a los hosts. Asegúrese de asociar los hosts ESXi a vCenter Server, y de configurar las listas de acceso y las listas de excepciones antes de configurar el modo de bloqueo.

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting DCUI.Access
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting DCUI.Access | Set-AdvancedSetting -Value root
```

Garantizar que el host ESXi tenga una lista precisa de usuarios con excepción

El host ESXi debe tener una lista precisa de usuarios con excepción.

Los usuarios de la lista de usuarios con excepción en modo de bloqueo no pierden sus privilegios cuando el host entra en modo de bloqueo. Esta situación podría anular el propósito del modo de bloqueo.

Valores

Valor predeterminado de instalación: nulo

Valor sugerido de línea base: nulo

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Posible pérdida de acceso administrativo a los hosts ESXi. Asegúrese de asociar los hosts ESXi a vCenter Server, y de configurar las listas de acceso y las listas de excepciones antes de configurar el modo de bloqueo.

Evaluación mediante comandos de PowerCLI

```
(Get-View (Get-VMHost -Name $ESXi | Get-
View).ConfigManager.HostAccessManager).QueryLockdownExceptions()
```

Ejemplo de corrección mediante un comando de PowerCLI

```
(Get-View (Get-VMHost -Name $ESXi | Get-
View).ConfigManager.HostAccessManager).UpdateLockdownExceptions($NULL)
```

Activar el modo de bloqueo normal para restringir el acceso a ESXi

Al activar el modo de bloqueo, se desactiva el acceso directo a un host ESXi. El modo de bloqueo requiere que vCenter Server administre el host ESXi directamente.

Restringir el acceso de esta manera garantiza que vCenter Server aplique funciones y permisos. Además, los usuarios no pueden omitir estas funciones y permisos al iniciar sesión en un host ESXi directamente. Requerir que toda la interacción se produzca a través de vCenter Server reduce el riesgo de que los usuarios obtengan privilegios altos inadvertidamente o realicen tareas para las que no se les realiza una auditoría correctamente.

Los usuarios que figuran en la lista de usuarios con excepción para cada host ESXi tienen permiso para anular el modo de bloqueo e iniciar sesión. De forma predeterminada, no hay usuarios presentes en la lista de usuarios con excepción.

Los ajustes del modo de bloqueo son Deshabilitado, Normal y Estricto. Cuando el modo de bloqueo se establece en Estricto, si el host ESXi pierde contacto con vCenter Server, no podrá administrarlo hasta que se restablezca la conexión. Si no puede restablecer la conexión, debe reconstruir el host ESXi. En general, el modo de bloqueo estricto supera las necesidades de la mayoría de las implementaciones. Por lo tanto, el modo de bloqueo normal suele ser suficiente.

Valores

Valor predeterminado de instalación: lockdownDisabled

Valor sugerido de línea base: lockdownNormal

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Posible pérdida de acceso administrativo a los hosts. Asegúrese de asociar los hosts ESXi a vCenter Server, y de configurar las listas de acceso y las listas de excepciones antes de configurar el modo de bloqueo.

Algunas operaciones, como la copia de seguridad y la solución de problemas, requieren acceso directo al host ESXi. En estos casos, puede desactivar el modo de bloqueo temporalmente para hosts específicos y, a continuación, volver a activar el modo de bloqueo cuando haya terminado.

Evaluación mediante comandos de PowerCLI

```
(Get-View (Get-VMHost -Name $ESXi | Get-View).ConfigManager.HostAccessManager).LockdownMode
```

Ejemplo de corrección mediante un comando de PowerCLI

```
(Get-View (Get-VMHost -Name $ESXi | Get-
View).ConfigManager.HostAccessManager).ChangeLockdownMode('lockdownNormal')
```

Syslog.global.auditRecord.storageEnable

Configura el host ESXi para almacenar los registros de auditoría de forma local.

Debe activar el registro de registros de auditoría en los hosts ESXi.

Valores

Valor predeterminado de instalación: False

Valor sugerido de línea base: true

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Los registros consumen espacio de almacenamiento adicional.

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Syslog.global.auditRecord.storageEnable
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Syslog.global.auditRecord.storageEnable | Set-
AdvancedSetting -Value TRUE
```

Syslog.global.auditRecord.storageCapacity

Debe activar la capacidad de almacenamiento durante una semana de los registros de auditoría en los hosts ESXi.

Si hay una instalación de almacenamiento de registros de auditoría remota disponible, es esencial garantizar que la capacidad de almacenamiento local sea suficiente para mantener los registros de auditoría que se pueden acumular durante las interrupciones previstas en la entrega de los registros a la instalación. Esto garantiza que los registros de auditoría no se pierdan ni se sobrescriban durante los períodos en los que el almacenamiento remoto no está disponible, lo que permite una continuidad sin problemas de la traza de auditoría y los requisitos de conformidad.

Valores

Valor predeterminado de la instalación: 4

Valor sugerido de línea base: 100

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Los registros consumen espacio de almacenamiento adicional.

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Syslog.global.auditRecord.storageCapacity
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Syslog.global.auditRecord.storageCapacity |
Set-AdvancedSetting -Value 100
```

ScratchConfig.CurrentScratchLocation y Syslog.global.auditRecord.storageDirectory

Configura una ubicación de registro persistente para todos los registros de auditoría almacenados localmente en el host ESXi.

Puede configurar ESXi para almacenar registros de auditoría en un sistema de archivos en la memoria. Esto ocurre cuando el directorio "/scratch" del host está vinculado a "/tmp/scratch". Cuando se hace esto, solo se almacenan registros de un solo día en cualquier momento. Además, los registros de auditoría se reinician después de cada reinicio. Esto representa un riesgo de seguridad, ya que la actividad del usuario que inició sesión en el host solo se almacena temporalmente y no se mantiene después del reinicio. Esto también puede complicar la auditoría, y dificultar la supervisión de eventos y el diagnóstico de problemas. Configure siempre el registro de auditoría del host ESXi en un almacén de datos persistente.

Puede detectar si el volumen de scratch es temporal o persistente al consultar la configuración avanzada de `ScratchConfig.CurrentScratchLocation`. Si, cuando se consulta, devuelve "/tmp/scratch", el volumen es temporal y debe volver a asignar el almacenamiento de registros de auditoría a un dispositivo persistente.

El almacenamiento no puede ser un almacén de datos de vSAN. Si el único almacenamiento local que no es de vSAN es un medio SD o USB (que puede volverse poco fiable con las escrituras repetidas de los registros), considere la posibilidad de dejar los registros en el disco RAM y asegúrese de que se haya configurado un host de registro remoto en su lugar. Documente la decisión y la lógica como preparación para futuras auditorías.

Valores

Valor predeterminado de instalación:

`ScratchConfig.CurrentScratchLocation`: depende del dispositivo de arranque.

`Syslog.global.auditRecord.storageDirectory`: `/scratch/auditLog`

Valor sugerido de línea base: ubicación de almacenamiento persistente

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Los registros consumen espacio de almacenamiento adicional.

Evaluación mediante comandos de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.syslog.config.get.Invoke() | Select
LocalLogOutput,LocalLogOutputIsPersistent

# If your LocalLogOutput is set to a directory in /scratch, and LocalLogOutputIsPersistent
is true, that means your boot device is of a type and size that makes /scratch persistent.
Verify that your audit storage is also on /scratch, and that /scratch points to a VMFS
datastore:
```

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting ScratchConfig.CurrentScratchLocation
Get-VMHost -Name $ESXi | Get-AdvancedSetting Syslog.global.auditRecord.storageDirectory
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Syslog.global.auditRecord.storageDirectory |
Set-AdvancedSetting -Value "/vmfs/volumes/$Datastore/audit"
```

Syslog.global.auditRecord.remoteEnable

Configura el host ESXi para la transmisión de registros de auditoría a un host remoto.

Valores

Valor predeterminado de instalación: False

Valor sugerido de línea base: true

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Syslog.global.auditRecord.remoteEnable
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Syslog.global.auditRecord.remoteEnable | Set-
AdvancedSetting -Value TRUE
```

Syslog.global.logFiltersEnable

Activa el filtro de registros en el host ESXi.

Puede crear filtros de registros para reducir la cantidad de entradas repetidas y denegar eventos de registros específicos en su totalidad.

Valores

Valor predeterminado de instalación: False

Valor sugerido de línea base: False

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Syslog.global.logFiltersEnable
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Syslog.global.logFiltersEnable | Set-
AdvancedSetting -Value FALSE
```

LocalLogOutputIsPersistent, ScratchConfig.CurrentScratchLocation y Syslog.global.logDir

Configura el registro persistente de todos los registros almacenados localmente en el host ESXi.

Puede configurar ESXi para almacenar archivos de registro en un sistema de archivos en la memoria. Esto ocurre cuando el directorio "/scratch" del host está vinculado a "/tmp/scratch". Cuando se hace esto, solo se almacenan los registros de un solo día en cualquier momento. Además, los archivos de registro se reinician después de cada reinicio. Esto representa un riesgo de seguridad, ya que la actividad del usuario que inició sesión en el host solo se almacena temporalmente y no se conserva después de los reinicios. También puede complicar la auditoría, y dificultar la supervisión de eventos y el diagnóstico de problemas. Configure siempre el registro del host ESXi en un almacén de datos persistente.

Puede detectar si el volumen de scratch es temporal o persistente al consultar el parámetro avanzado de `ScratchConfig.CurrentScratchLocation`. Si, cuando se consulta, devuelve "/tmp/scratch", el volumen es temporal y debe volver a asignar el almacenamiento de registros de auditoría a un dispositivo persistente.

El almacenamiento no puede ser un almacén de datos de vSAN, a menos que establezca `Syslog.global.vsanBacking`, que tiene advertencias y dependencias. Si el único almacenamiento local que no es de vSAN es un medio SD o USB (que puede volverse poco fiable con las escrituras repetidas de los registros), considere la posibilidad de dejar los registros en el disco RAM y asegúrese de que se haya configurado un host de registro remoto en su lugar. Documente la decisión y la lógica como preparación para futuras auditorías.

Valores

Valor predeterminado de instalación: `ScratchConfig.CurrentScratchLocation`: depende del dispositivo de arranque.

`Syslog.global.logDir`: `/scratch/log`

Valor sugerido de línea base: ubicación de almacenamiento persistente

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.syslog.config.get.Invoke() | Select
LocalLogOutput,LocalLogOutputIsPersistent

# If your LocalLogOutput is set to a directory in /scratch, and LocalLogOutputIsPersistent
is true, that means your boot device is of a type and size that makes /scratch persistent.
Verify that your log storage is also on /scratch, , and that /scratch points to a VMFS
datastore:

Get-VMHost -Name $ESXi | Get-AdvancedSetting ScratchConfig.CurrentScratchLocation
Get-VMHost -Name $ESXi | Get-AdvancedSetting Syslog.global.logDir
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Syslog.global.logDir | Set-AdvancedSetting
-Value "/vmfs/volumes/$Datastore/logs"
```

Syslog.global.logHost

Configura el registro remoto.

Cuando configura el registro remoto en un host de registro central, proporciona un almacén centralizado y seguro para los registros de ESXi. La recopilación de archivos de registro del host en un host central permite supervisar todos los hosts con una sola herramienta. También puede realizar análisis adicionales y buscar elementos como ataques coordinados en varios hosts. El inicio de sesión en un servidor de registro centralizado y seguro ayuda a prevenir la modificación de los registros, además de proporcionar un registro de auditoría a largo plazo.

Valores

Valor predeterminado de instalación: no definido

Valor sugerido de línea base: específico del sitio

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Syslog.global.logHost
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Syslog.global.logHost | Set-AdvancedSetting
-Value "log_collector"
```

Syslog.global.certificate.checkSSLCerts

Comprueba los certificados de TLS.

El host ESXi debe comprobar los certificados de los endpoints de registro remoto de TLS. Los certificados de TLS garantizan que el endpoint sea auténtico y confiable.

Valores

Valor predeterminado de instalación: True

Valor sugerido de línea base: true

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Syslog.global.certificate.checkSSLCerts
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Syslog.global.certificate.checkSSLCerts | Set-
AdvancedSetting -Value TRUE
```

Syslog.global.certificate.strictX509Compliance

Realiza una verificación x509 estricta para los endpoints de registro remoto habilitados para TLS.

El host ESXi debe utilizar una verificación x509 estricta para los endpoints de registro remoto habilitados para TLS. La configuración de `Syslog.global.certificate.strictX509Compliance` realiza comprobaciones de validez adicionales en los certificados raíz de CA durante la verificación.

Valores

Valor predeterminado de instalación: False

Valor sugerido de línea base: true

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Syslog.global.certificate.strictX509Compliance
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting
Syslog.global.certificate.strictX509Compliance | Set-AdvancedSetting -Value TRUE
```

Mem.MemEagerZero

Activa la destrucción de claves volátiles.

De forma predeterminada, ESXi coloca en cero las páginas asignadas para máquinas virtuales, las aplicaciones del espacio del usuario y los subprocesos de kernel en el momento de la asignación. Esto garantiza que no se expongan páginas que no estén en cero a las máquinas virtuales ni a las aplicaciones del espacio del usuario. Esta medida se aplica para evitar la exposición de claves criptográficas de máquinas virtuales o ámbitos del usuario a otros clientes.

Sin embargo, si no se reutiliza la memoria, estas claves pueden permanecer presentes en la memoria del host durante un período prolongado. Para solucionar esto, puede configurar el ajuste de `MemEagerZero` para aplicar la puesta a cero de las páginas de memoria del ámbito del usuario y del invitado cuando un invitado o un proceso del ámbito del usuario salga. En el caso de los subprocesos del kernel, los espacios de memoria que contienen claves se ponen en cero tan pronto como ya no se requiere el secreto.

Valores

Valor predeterminado de instalación: 0

Valor sugerido de línea base: 1

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Se requiere de un tiempo de apagado adicional para las máquinas virtuales, que corresponde a la cantidad de memoria asignada.

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Mem.MemEagerZero
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Mem.MemEagerZero | Set-AdvancedSetting -Value
1
```

Comprobar el mantenimiento activo en la versión de ESXi

Asegúrese de que la versión de ESXi no esté en el estado Fin de soporte general de VMware.

Valores

Valor predeterminado de instalación: N/D

Valor sugerido de línea base: N/D

Acción necesaria

Audite la versión de ESXi periódicamente.

Impacto funcional potencial si se cambia el valor predeterminado

Lea siempre las Notas de la versión, y pruebe e implemente nuevas versiones de software mediante implementaciones graduales.

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Select-Object Name,Version,Build
```

Ejemplo de corrección mediante un comando de PowerCLI

N/C

Activar los orígenes de la sincronización de hora

El host ESXi debe tener servicios de sincronización de hora activados y en ejecución.

La criptografía, el registro de auditoría, las operaciones del clúster y la respuesta a incidentes y los análisis se basan en la sincronización de la hora. Para garantizar que la hora esté sincronizada en todos los servicios y las operaciones, active los servicios NTP o PTP para que comiencen con el host y asegúrese de que dichos servicios se estén ejecutando.

Valores

Valor predeterminado de instalación: Detenido, Iniciar y detener manualmente

Valor sugerido de línea base: Ejecutar, Detener e iniciar con el host

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VMHostService -VMHost $ESXi | Where-Object{$_.Key -eq "ntpd"}
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHostService -VMHost $ESXi -ErrorAction:Stop | Where-Object{$_.Key -eq "ntpd"} | Set-
VMHostService -policy "on" -Confirm:$false
Get-VMHostService -VMHost $ESXi -ErrorAction:Stop | Where-Object{$_.Key -eq "ntpd"} |
Restart-VMHostService -Confirm:$false
```

Configurar orígenes de sincronización de hora confiables

El host ESXi debe tener configurados los orígenes de sincronización de hora confiables.

La criptografía, el registro de auditoría, las operaciones del clúster y la respuesta a incidentes y los análisis dependen de la sincronización de la hora. El protocolo de tiempo de red (NTP) debe tener al menos cuatro orígenes. Si debe elegir entre dos orígenes y un origen, es preferible uno solo.

El protocolo de hora de precisión (PTP) es una alternativa a NTP que proporciona una precisión temporal de submilisegundos. La arquitectura de PTP es diferente de la de NTP y no tiene la misma resistencia a los errores del servidor principal. Considere la posibilidad de configurar el NTP como un origen de copia de seguridad del PTP, de modo que un origen de hora siga estando disponible, incluso si la precisión es menor.

Valores

Valor predeterminado de instalación: no definido

Valor sugerido de línea base:

Específico del sitio o:

0.vmware.pool.ntp.org,

1.vmware.pool.ntp.org,

2.vmware.pool.ntp.org,

3.vmware.pool.ntp.org

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VMHostNtpServer -VMHost $ESXi
```

Ejemplo de corrección mediante un comando de PowerCLI

```
$ntp0 = "0.vmware.pool.ntp.org"
$ntp1 = "1.vmware.pool.ntp.org"
$ntp2 = "2.vmware.pool.ntp.org"
$ntp3 = "3.vmware.pool.ntp.org"

Add-VMHostNTPServer -NtpServer $ntp0 , $ntp1 , $ntp2 , $ntp3 -VMHost $ESXi -Confirm:$false
```

Usar cifrados TLS

El host ESXi debe mantener la confidencialidad y la integridad de las transmisiones mediante la habilitación de cifrados TLS modernos.

A partir de ESXi 8.0 Update 3, los perfiles de TLS configuran los ajustes de TLS del cliente y del servidor para que solo usen cifrados seguros. Puede ver toda la lista y los conjuntos de claves de cifrado mediante los siguientes comandos:

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.system.tls.server.get.CreateArgs()
$arguments.showprofiledefaults = $true
$arguments.showcurrentbootprofile = $true
$ESXcli.system.tls.server.get.invoke($arguments)
```

Debe reiniciar el host ESXi después de realizar cambios en el perfil de TLS. (En vSphere Client, el host presenta el sufijo de "Reinicio necesario").

Valores

Valor predeterminado de instalación: COMPATIBILE

Valor sugerido de línea base: NIST_2024

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Los cambios en los conjuntos de claves de cifrado afectan la conectividad con sistemas externos. Debe reiniciar el host para que se aplique este cambio de perfil de TLS.

Evaluación mediante comandos de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.tls.server.get.invoke() | Select-Object -ExpandProperty Profile
```

Ejemplo de corrección mediante un comando de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.system.tls.server.set.CreateArgs()
$arguments.profile = "NIST_2024"
$ESXcli.system.tls.server.set.invoke($arguments)
```

UserVars.ESXiVPsDisabledProtocols

El host ESXi debe habilitar la versión más alta de TLS admitida.

ESXi 8.0 activa TLS 1.2 de forma predeterminada, pero es posible activar otros protocolos si es necesario. A partir de ESXi 8.0 Update 3, TLS 1.3 está activado de forma predeterminada.

Valores

Valor predeterminado de instalación: sslv3,tlsv1,tlsv1.1

Valor sugerido de línea base: sslv3,tlsv1,tlsv1.1

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting UserVars.ESXiVPsDisabledProtocols
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting UserVars.ESXiVPsDisabledProtocols | Set-
AdvancedSetting -Value "sslv3,tlsv1,tlsv1.1"
```

Configurar el cifrado basado en TPM

El host ESXi debe requerir un cifrado de configuración basado en TPM.

La configuración de un host ESXi consta de archivos de configuración para cada servicio que se ejecuta en el host. Los archivos de configuración suelen residir en el directorio `/etc`, pero también pueden residir en otros espacios de nombres. Los archivos de configuración contienen información en tiempo de ejecución sobre el estado de los servicios. Con el tiempo, los valores predeterminados de los archivos de configuración pueden cambiar, por ejemplo, cuando se cambia la configuración en el host ESXi.

Un trabajo cron realiza una copia de seguridad de los archivos de configuración de ESXi periódicamente, o cuando ESXi se apaga correctamente o a pedido, y crea un archivo de configuración archivado en el banco de arranque. Cuando ESXi se reinicia, el sistema lee el archivo de configuración archivado y vuelve a crear el estado en el que ESXi estaba cuando se creó la copia de seguridad.

Antes de vSphere 7.0 Update 2, el archivo de configuración ESXi archivado no está cifrado. En vSphere 7.0 Update 2 y versiones posteriores, se cifra el archivo de configuración archivado. Cuando el host ESXi está configurado con un módulo de plataforma de confianza (TPM), el TPM se utiliza para "sellar" la configuración en el host, lo que proporciona una garantía de seguridad sólida y protección adicional contra los ataques sin conexión.

El cifrado de configuración utiliza el TPM físico cuando está disponible y se admite en el momento de la instalación o la actualización. Si el TPM se agregó o se habilitó más adelante, debe volver a configurar explícitamente el host ESXi para utilizar el TPM recién disponible. Una vez habilitado el cifrado de la configuración de TPM, no se puede desactivar.

Valores

Valor predeterminado de instalación: específico del sitio

Valor sugerido de línea base: TPM

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

El uso del arranque seguro y el cifrado de configuración forzado por TPM hacen inutilizables los esfuerzos tradicionales de recuperación de la contraseña raíz. Asegúrese de no perder el acceso a las cuentas del administrador ESXi.

Evaluación mediante comandos de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.settings.encryption.get.Invoke() | Select Mode
```

Ejemplo de corrección mediante un comando de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.system.settings.encryption.set.CreateArgs()
```

```
$arguments.mode = "TPM"
$ESXcli.system.settings.encryption.set.Invoke($arguments)
```

Comprobar que el software ESXi esté actualizado

Al mantenerse al día con las revisiones ESXi, se mitigan las vulnerabilidades en el hipervisor.

Un atacante con formación puede aprovechar las vulnerabilidades conocidas al intentar acceder o elevar los privilegios en un host ESXi. Actualice siempre vCenter Server primero; si hay una actualización disponible, y luego actualice ESXi.

Valores

Valor predeterminado de instalación: Downlevel

Valor sugerido de línea base: Actual

Acción necesaria

Audite periódicamente el nivel de revisión ESXi.

Lea siempre las Notas de la versión, y pruebe e implemente nuevas versiones de software mediante implementaciones graduales.

Impacto funcional potencial si se cambia el valor predeterminado

Las versiones de actualización de vSphere Update agregan y cambian la funcionalidad. Las versiones de revisión solo resuelven problemas.

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Select-Object Name,Version,Build
```

Ejemplo de corrección mediante un comando de PowerCLI

N/C

VMkernel.Boot.execInstalledOnly

Ejecute archivos binarios que solo entregue un VIB.

ESXi realiza comprobaciones de integridad de los VIB en función del nivel de aceptación. Indicar a ESXi que solo ejecute archivos binarios que se originen a partir de un VIB válido instalado en el host hace que sea más difícil para los atacantes utilizar kits de herramientas precompilados durante un riesgo, y aumenta las posibilidades de detección.

Valores

Valor predeterminado de instalación: False

Valor sugerido de línea base: true

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Es posible que el software no firmado de terceros no se instale ni se ejecute.

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting VMkernel.Boot.execInstalledOnly
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting VMkernel.Boot.execInstalledOnly | Set-
AdvancedSetting -Value True
```

Desactivar los servicios de administración en adaptadores de VMkernel

Asegúrese de que vSAN, vMotion y otros adaptadores de VMkernel dedicados no tengan los servicios de administración activados.

Las interfaces de red de VMkernel que están destinadas a un uso especializado pueden configurarse con capacidades de administración, lo que podría anular los esfuerzos de seguridad y aislamiento de red. Habilite solo los servicios de administración en las interfaces de VMkernel destinadas a la administración.

Valores

Valor predeterminado de instalación: específico del sitio

Valor sugerido de línea base: específico del sitio

Acción necesaria

Audite los valores específicos del sitio.

Impacto funcional potencial si se cambia el valor predeterminado

Es posible que algunas soluciones administradas de terceros requieran que se activen los servicios de administración en los adaptadores de Vmkernel.

Evaluación mediante comandos de PowerCLI

```
Get-VMHostNetworkAdapter -VMHost $ESXi -VMKernel | Select
VMHost,Name,IP,ManagementTrafficEnabled
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHostNetworkAdapter -VMHost $ESXi -Name $vmkernel_interface | Set-
VMHostNetworkAdapter -ManagementTrafficEnabled $false
```

Configurar el firewall ESXi para bloquear el tráfico

Debe configurar el firewall del host ESXi para bloquear el tráfico de red de forma predeterminada.

Asegúrese de que todo el tráfico de red entrante y saliente esté bloqueado, a menos que se permita explícitamente, lo que reduce la superficie de ataque y evita el acceso no autorizado al host.

Valores

Valor predeterminado de instalación: activado

Valor sugerido de línea base: activado

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

El firewall es simplista, similar a las LCA del enrutador. Es posible que deba volver a configurar las reglas reflexivas.

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Get-VMHostFirewallDefaultPolicy
```

Ejemplo de corrección mediante un comando de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.network.firewall.set.CreateArgs()
$arguments.defaultaction = $FALSE
$arguments.enabled = $true
$ESXcli.network.firewall.set.Invoke($arguments)
```

Configurar el firewall de ESXi para redes autorizadas

Configure el firewall de ESXi para permitir el tráfico solo desde redes autorizadas.

Asegúrese de que todo el tráfico de red entrante y saliente esté bloqueado, a menos que se permita explícitamente, lo que reduce la superficie de ataque y evita el acceso no autorizado al host ESXi.

A partir de vSphere 8.0 Update 2, las reglas de firewall se clasifican como propiedad de "usuario" o "sistema", donde solo se pueden configurar las reglas que son propiedad del "usuario". En vSphere 8 Update 2b y PowerCLI 13.2.1, hay parámetros adicionales a los que se puede consultar para automatizar la configuración y la comprobación de las reglas configurables.

Valores

Valor predeterminado de instalación: conexiones permitidas desde cualquier dirección IP

Valor sugerido de línea base: solo se permiten conexiones desde estaciones de trabajo de infraestructura y administración autorizadas

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

El firewall es simplista, similar a las LCA del enrutador. Es posible que deba volver a configurar las reglas reflexivas.

Evaluación mediante comandos de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$list = $ESXcli.network.firewall.ruleset.list.Invoke() | Where {($_.AllowedIPconfigurable
-eq $true) -and ($_.EnableDisableconfigurable -eq $true)} | Select -ExpandProperty Name

$arguments = $ESXcli.network.firewall.ruleset.allowedip.list.CreateArgs()
foreach ($rule in $list) {
    $arguments.rulesetid = $rule
    $ESXcli.network.firewall.ruleset.allowedip.list.Invoke($arguments)
}
```

Ejemplo de corrección mediante un comando de PowerCLI

```
# Customize this example for your environment.
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
# Deactivate firewall temporarily so we don't lose connectivity
$arguments = $ESXcli.network.firewall.set.CreateArgs()
$arguments.enabled = $false
$ESXcli.network.firewall.set.Invoke($arguments)

# Unset the "allow all" flag
$arguments = $ESXcli.network.firewall.ruleset.set.CreateArgs()
$arguments.allowedall = $false
$arguments.rulesetid = "sshServer"
$ESXcli.network.firewall.ruleset.set.Invoke($arguments)

# Add an IP range
$arguments = $ESXcli.network.firewall.ruleset.allowedip.add.CreateArgs()
```

```
$arguments.ipaddress = "192.168.0.0/16"
$arguments.rulesetid = "sshServer"
$ESXcli.network.firewall.ruleset.allowedip.add.Invoke($arguments)

# Enable the firewall
$arguments = $ESXcli.network.firewall.set.CreateArgs()
$arguments.enabled = $true
$ESXcli.network.firewall.set.Invoke($arguments)
```

Configurar la directiva de transmisiones falsificadas en Rechazar

Configure la directiva de transmisiones falsificadas en Rechazar tanto en el conmutador estándar de vSphere como en sus grupos de puertos.

Si el sistema operativo de la máquina virtual cambia la dirección MAC, el sistema operativo puede enviar marcos con una dirección MAC de origen suplantada en cualquier momento. La suplantación de direcciones MAC permite que un sistema operativo realice ataques maliciosos en los dispositivos de una red suplantando un adaptador de red autorizado por la red receptora. Cuando la directiva de transmisiones falsificadas está establecida en Aceptar, ESXi no compara las direcciones MAC de origen y efectivas. Para evitar la suplantación de MAC, configure la directiva Transmisiones falsificadas en Rechazar. El host luego compara la dirección MAC de origen que transmite el sistema operativo invitado con la dirección MAC efectiva del adaptador de la máquina virtual para ver si coinciden. Si las direcciones no coinciden, el host ESXi descarta el paquete.

Valores

Valor predeterminado de instalación: Aceptar

Valor sugerido de línea base: Rechazar

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Algunas cargas de trabajo, como las aplicaciones agrupadas en clúster y los dispositivos de red y las funciones, dependen de estas técnicas como una parte normal de su funcionamiento. Si es necesario, puede configurar un grupo de puertos independiente que permita este comportamiento y asociarle solo máquinas virtuales autorizadas.

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Get-VirtualSwitch -Standard | Get-SecurityPolicy | select 
VirtualSwitch,ForgedTransmits
```

```
Get-VMHost -Name $ESXi | Get-VirtualPortGroup -Standard | Get-SecurityPolicy | select
VirtualPortGroup,ForgedTransmits
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHost -Name $ESXi | Get-VirtualSwitch -Standard | Get-SecurityPolicy | Set-
SecurityPolicy -ForgedTransmits $false
Get-VMHost -Name $ESXi | Get-VirtualPortGroup -Standard | Get-SecurityPolicy | Set-
SecurityPolicy -ForgedTransmitsInherited $true
```

Establecer la directiva de cambios de dirección MAC en Rechazar

Establezca la directiva de cambios de dirección MAC en Rechazar tanto en el conmutador estándar de vSphere como en sus grupos de puertos.

Si el sistema operativo de la máquina virtual cambia la dirección MAC, puede enviar marcos con una dirección MAC de origen suplantada, lo que le permite realizar ataques malintencionados en los dispositivos dentro de una red al suplantar un adaptador de red autorizado por la red receptora. Para evitar que las máquinas virtuales cambien su dirección MAC efectiva, se deben tomar medidas para aplicar la estabilidad de la dirección MAC o restringir la capacidad de modificar direcciones MAC. Esto mitiga el riesgo de suplantación de MAC y las posibles actividades malintencionadas.

Valores

Valor predeterminado de instalación: Aceptar

Valor sugerido de línea base: Rechazar

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Algunas cargas de trabajo, como las aplicaciones agrupadas en clúster, las funciones y los dispositivos de red, las aplicaciones con licencia por dirección MAC y la actualización con periodo de inactividad reducido de vCenter Server, dependen de estas técnicas como parte normal de su funcionamiento. Si es necesario, puede configurar un grupo de puertos independiente que permita este comportamiento y asociarle solo máquinas virtuales autorizadas.

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Get-VirtualSwitch -Standard | Get-SecurityPolicy | select
VirtualSwitch,MacChanges
```

```
Get-VMHost -Name $ESXi | Get-VirtualPortGroup -Standard | Get-SecurityPolicy | select
VirtualPortGroup,MacChanges
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHost -Name $ESXi | Get-VirtualSwitch -Standard | Get-SecurityPolicy | Set-
SecurityPolicy -MacChanges $false
Get-VMHost -Name $ESXi | Get-VirtualPortGroup -Standard | Get-SecurityPolicy | Set-
SecurityPolicy -MacChangesInherited $true
```

Establecer la directiva de modo promiscuo en Rechazar

Establezca la directiva de modo promiscuo en Rechazar tanto en el conmutador estándar de vSphere como en sus grupos de puertos.

Cuando se habilita el modo promiscuo en un grupo de puertos, todas las máquinas virtuales conectadas a ese grupo de puertos tienen la posibilidad de leer todos los paquetes transmitidos a través de ese grupo de puertos, independientemente del destinatario previsto. Tenga en cuenta el impacto potencial y las consideraciones de diseño antes de cambiar el valor predeterminado del modo promiscuo.

Valores

Valor predeterminado de instalación: Rechazar

Valor sugerido de línea base: Rechazar

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ciertas cargas de trabajo y tipos de trabajo, como los servidores DHCP, los dispositivos de red y la supervisión de seguridad, incorporan estas técnicas como parte regular de su funcionamiento. Si es necesario, puede configurar un grupo de puertos independiente que permita este comportamiento y asociarle solo máquinas virtuales autorizadas.

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Get-VirtualSwitch -Standard | Get-SecurityPolicy | select
VirtualSwitch,AllowPromiscuous
Get-VMHost -Name $ESXi | Get-VirtualPortGroup -Standard | Get-SecurityPolicy | select
VirtualPortGroup,AllowPromiscuous
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHost -Name $ESXi | Get-VirtualSwitch -Standard | Get-SecurityPolicy | Set-
SecurityPolicy -AllowPromiscuous $false
```

```
Get-VMHost -Name $ESXi | Get-VirtualPortGroup -Standard | Get-SecurityPolicy | Set-
SecurityPolicy -AllowPromiscuousInherited $true
```

Restringir el etiquetado de invitado virtual en conmutadores estándar

El host ESXi debe restringir el uso del etiquetado de invitado virtual (Virtual Guest Tagging, VGT) en los conmutadores estándar.

Cuando un grupo de puertos se establece en VLAN 4095, el vSwitch pasa todas las tramas de red a las máquinas virtuales asociadas sin modificar las etiquetas de VLAN. En vSphere, esto se conoce como VGT. La máquina virtual debe procesar la información de VLAN mediante un controlador 802.1Q en el sistema operativo.

VLAN 4095 solo debe implementarse si las máquinas virtuales asociadas tienen autorización específica y son capaces de administrar las etiquetas de VLAN por sí mismas. Si VLAN 4095 está habilitado de forma inadecuada, puede provocar una denegación del servicio o permitir que una máquina virtual interactúe con el tráfico en una VLAN no autorizada.

Valores

Valor predeterminado de instalación: no VLAN 4095

Valor sugerido de línea base: no VLAN 4095

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Get-VirtualPortGroup -Standard | select Name,VlanID
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHost -Name $ESXi | Get-VirtualPortGroup -Standard -Name $PG| Set-VirtualPortGroup
-VlanID "new_VLAN"
```

Activar la aplicación del arranque seguro

El arranque seguro forma parte del estándar del firmware UEFI. Con el arranque seguro UEFI activado, un host ESXi se niega a cargar cualquier aplicación o controlador UEFI, a menos que el cargador de arranque del sistema operativo tenga una firma digital válida. El arranque seguro de ESXi requiere la compatibilidad del firmware. El arranque seguro de ESXi también requiere que todos los módulos de kernel, los controladores y los VIB de ESXi estén firmados por VMware o un subordinado del socio.

El arranque seguro se activa en el BIOS del servidor físico ESXi y es compatible con el cargador de arranque del hipervisor. Este control cambia ESXi de simplemente admitir el arranque seguro a requerirlo. Sin esta configuración activada y sin el cifrado de la configuración, un host ESXi podría estar sujeto a ataques sin conexión. Un atacante simplemente podría transferir la unidad de instalación de ESXi a un host de arranque no seguro y realizar el arranque.

Valores

Valor predeterminado de instalación: False

Valor sugerido de línea base: true

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

El uso del arranque seguro y el cifrado de configuración forzado por TPM hacen inutilizables los esfuerzos tradicionales de recuperación de la contraseña raíz. Asegúrese de no perder el acceso a las cuentas del administrador ESXi.

Evaluación mediante comandos de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.settings.encryption.get.Invoke() | Select RequireSecureBoot
```

Ejemplo de corrección mediante un comando de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.system.settings.encryption.set.CreateArgs()
$arguments.requiresecureboot = $true
$ESXcli.system.settings.encryption.set.Invoke($arguments)
```

Desactivar ESXi Shell

ESXi Shell debe desactivarse.

Valores

Valor predeterminado de instalación: Detenido, Iniciar y detener manualmente

Valor sugerido de línea base: Detenido, Iniciar y detener manualmente

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VMHostService -VMHost $ESXi | Where-Object {$_.Key -eq 'TSM' -and $_.Running -eq
'True'}
Get-VMHostService -VMHost $ESXi | Where-Object {$_.Key -eq 'TSM' -and $_.Policy -eq 'On'}
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHostService -VMHost $ESXi | where {$_.Key -eq 'TSM'} | Set-VMHostService -Policy Off
Get-VMHostService -VMHost $ESXi | where {$_.Key -eq 'TSM'} | Stop-VMHostService
```

UserVars.ESXiShellInteractiveTimeOut

Establece un tiempo de espera para finalizar automáticamente las sesiones de ESXi Shell y de SSH inactivas.

Si los usuarios se olvidan de cerrar la sesión de SSH, la conexión inactiva permanece abierta de forma indefinida, lo que aumenta la posibilidad de que otros usuarios obtengan acceso privilegiado al host. Puede configurar las sesiones de shell inactivas para que finalicen automáticamente.

Valores

Valor predeterminado de instalación: 0

Valor sugerido de línea base: 900

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting UserVars.ESXiShellInteractiveTimeOut
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting UserVars.ESXiShellInteractiveTimeOut | Set-
AdvancedSetting -Value 900
```

Desactivar el servicio de SNMP

Desactive el servicio de SNMP si no lo está utilizando.

Valores

Valor predeterminado de instalación: Detenido, Iniciar y detener con el host

Valor sugerido de línea base: Detenido, Iniciar y detener manualmente

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VMHostService -VMHost $ESXi | Where-Object {$_.Key -eq 'snmpd' -and $_.Running -eq
'True'}
Get-VMHostService -VMHost $ESXi | Where-Object {$_.Key -eq 'snmpd' -and $_.Policy -eq 'On'}
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHostService -VMHost $ESXi | where {$_.Key -eq 'snmpd'} | Set-VMHostService -Policy
Off
Get-VMHostService -VMHost $ESXi | where {$_.Key -eq 'snmpd'} | Stop-VMHostService
```

Desactivar el servicio de SSH

Desactive el SSH y actívelo solo para solucionar problemas.

ESXi no es un sistema operativo multiusuario similar a UNIX. ESXi es un hipervisor diseñado para que lo administren VMware Host Client, vSphere Client, las CLI y las API. En ESXi, SSH es una interfaz de solución de problemas y soporte, y se detiene y desactiva intencionalmente de forma predeterminada. La activación de la interfaz conlleva riesgos.

Valores

Valor predeterminado de instalación: Detenido, Iniciar y detener manualmente

Valor sugerido de línea base: Detenido, Iniciar y detener manualmente

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VMHostService -VMHost $ESXi | Where-Object {$_.Key -eq 'TSM-SSH' -and $_.Running -eq
'True'}
```

```
Get-VMHostService -VMHost $ESXi | Where-Object {$_.Key -eq 'TSM-SSH' -and $_.Policy -eq
'On'}
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHostService -VMHost $ESXi | where {$_.Key -eq 'TSM-SSH'} | Set-VMHostService -Policy
Off
Get-VMHostService -VMHost $ESXi | where {$_.Key -eq 'TSM-SSH'} | Stop-VMHostService
```

Usar entropía para las operaciones criptográficas

El host ESXi debe utilizar suficiente entropía para las operaciones criptográficas.

En vSphere 8.0 y versiones posteriores, la implementación de la entropía de ESXi admite las certificaciones FIPS 140-3 y EAL4. Las opciones de arranque del kernel controlan qué orígenes de entropía se activan en un host ESXi.

Valores

Valor predeterminado de instalación:

disableHwrng = FALSE

entropySources = 0

Valor sugerido de línea base:

disableHwrng = FALSE

entropySources = 0

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.settings.kernel.list.Invoke() | Where {$_.Name -eq "disableHwrng" -or
$_.Name -eq "entropySources"}
```

Ejemplo de corrección mediante un comando de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.system.settings.kernel.set.CreateArgs()
$arguments.setting = "disableHwrng"
$arguments.value = "FALSE"
$ESXcli.system.settings.kernel.set.invoke($arguments)
$arguments.setting = "entropySources"
```

```
$arguments.value = "0"
$ESXcli.system.settings.kernel.set.invoke($arguments)
```

Comprobar el perfil de imagen y los niveles de aceptación de VIB

El nivel de aceptación del perfil de imagen del host ESXi debe ser PartnerSupported o superior.

El nivel de aceptación controla lo que ESXi permite que se instale. Consulte Administrar los niveles de aceptación de los hosts ESXi y los paquetes de instalación de vSphere para conocer los niveles de VIB.

Ni VMware ni los socios de VMware prueban los VIB CommunitySupported, ni los VIB CommunitySupported contienen una firma digital. Por estos motivos, tenga cuidado al instalar los VIB CommunitySupported.

Valores

Valor predeterminado de instalación: PartnerSupported

Valor sugerido de línea base: PartnerSupported o superior

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Los paquetes CommunitySupported no están firmados y no se pueden instalar.

Evaluación mediante comandos de PowerCLI

```
(Get-EsxCli -VMHost $ESXi -V2).software.acceptance.get.Invoke()
```

Ejemplo de corrección mediante un comando de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.software.acceptance.set.CreateArgs()
$arguments.level = "PartnerSupported" # VMwareCertified, VMwareAccepted, PartnerSupported, 
CommunitySupported
$ESXcli.software.acceptance.set.Invoke($arguments)
```

Security.AccountUnlockTime

El host ESXi debe desbloquear las cuentas después de un tiempo de espera especificado.

`Security.AccountUnlockTime` garantiza que las cuentas de usuario del host ESXi se desbloqueen automáticamente después de un periodo definido de inactividad. Al aplicar el desbloqueo automático de cuentas, las organizaciones pueden mantener un equilibrio entre la seguridad y la capacidad de uso, lo que garantiza que las cuentas inactivas se reactiven con rapidez, a la vez que se minimiza la posibilidad de acceso no autorizado.

Valores

Valor predeterminado de instalación: 900 segundos

Valor sugerido de línea base: 900 segundos

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Security.AccountUnlockTime
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Security.AccountUnlockTime | Set-
AdvancedSetting -Value 900
```

Security.AccountLockFailures

Establece el recuento máximo de intentos de inicio de sesión fallidos antes de bloquear la cuenta.

Brinda protección contra ataques por fuerza bruta e intentos de acceso no autorizado al deshabilitar temporalmente la cuenta afectada, lo que evita que se produzcan más intentos de inicio de sesión hasta que el periodo de bloqueo caduque o un administrador lo restablezca manualmente. Para desbloquear una cuenta bloqueada, es necesario realizar una acción administrativa o esperar a que la cuenta se desbloquee de forma automática si se utiliza la configuración de `Security.AccountUnlockTime`.

Valores

Valor predeterminado de instalación: 5

Valor sugerido de línea base: 5

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Un umbral bajo para errores de inicio de sesión puede aumentar los ataques de denegación del servicio, ya sean intencionales o accidentales, como con reintentos de conexión SSH.

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Security.AccountLockFailures
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Security.AccountLockFailures | Set-
AdvancedSetting -Value 5
```

Security.PasswordHistory

No permite la reutilización de contraseñas.

Esta opción evita la reutilización de contraseñas anteriores, lo que mitiga las posibles infracciones por credenciales antiguas y vulneradas.

Valores

Valor predeterminado de instalación: 5

Valor sugerido de línea base: 5

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Security.PasswordHistory
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Security.PasswordHistory | Set-
AdvancedSetting -Value 5
```

Security.PasswordMaxDays

Establece el número máximo de días entre cambios de contraseña.

Las prácticas recomendadas modernas para contraseñas, tal como se describe en la sección 5.1.1.2 de NIST 800-63B y otras guías relevantes, indican que la aplicación de cambios periódicos de contraseñas no mejora la seguridad cuando las contraseñas ya poseen una entropía adecuada.

Valores

Valor predeterminado de instalación: 99999

Valor sugerido de línea base: 99999

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Security.PasswordMaxDays
```

Comando PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Security.PasswordMaxDays | Set-
AdvancedSetting -Value 99999
```

Security.PasswordQualityControl

Exige la complejidad de la contraseña.

En las recomendaciones como la Sección 5.1.1.2 de NIST 800-63B se sugiere que las reglas de composición, por ejemplo, que exigen mezclas de clases de caracteres, no deben aplicarse en los sistemas, ya que a menudo no mejoran la seguridad de las contraseñas y desalientan la adopción de frases de contraseña más seguras.

Las reglas de seguridad y complejidad de contraseñas se aplican a todos los usuarios ESXi, incluido el usuario raíz. Sin embargo, cuando el host ESXi está unido a un dominio, estas reglas no se aplican a los usuarios de Active Directory (AD), ya que el sistema de AD aplica las directivas de contraseña para los usuarios de AD.

Valores

Valor predeterminado de instalación: retry=3 min=disabled,disabled,disabled,7,7

Valor sugerido de línea base: retry=3 min=disabled,15,15,15,15 max=64 similar=deny passphrase=3

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Es posible que otros productos y servicios dentro del ecosistema de VMware no esperen cambios en los requisitos de complejidad de la contraseña y se produzca un error en la instalación.

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Security.PasswordQualityControl
```

Comando PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Security.PasswordQualityControl | Set-
AdvancedSetting -Value "retry=3 min=disabled,15,15,15,15 max=64 similar=deny passphrase=3"
```

UserVars.SuppressHyperthreadWarning

Suprime la advertencia de una posible vulnerabilidad de seguridad de hiperproceso.

Las advertencias de seguridad del hiperproceso significan vulnerabilidades de CPU no atendidas en el sistema. Ignorar estas advertencias podría enmascarar posibles riesgos. Asegúrese de que las correcciones de hardware correspondan con el riesgo aceptado de su organización. Cuando elimine una advertencia, documente la decisión y la justificación.

Valores

Valor predeterminado de instalación: 0

Valor sugerido de línea base: 0

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting UserVars.SuppressHyperthreadWarning
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting UserVars.SuppressHyperthreadWarning | Set-
AdvancedSetting -Value 0
```

UserVars.DcuiTimeOut

Establece un tiempo de espera para finalizar de forma automática las sesiones de DCUI inactivas.

La DCUI permite el inicio de sesión directo en el host ESXi para las tareas de administración. Para evitar el uso no intencionado de la DCUI de sesiones de inicio de sesión sobrantes, finalice las conexiones inactivas.

Valores

Valor predeterminado de instalación: 600

Valor sugerido de línea base: 600

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting UserVars.DcuiTimeOut
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting UserVars.DcuiTimeOut | Set-AdvancedSetting
-Value 600
```

Desactivar el servicio de CIM

El servicio de CIM ESXi debe desactivarse.

Los servicios que no están en uso y que no son esenciales para las operaciones deben desactivarse.

Valores

Valor predeterminado de instalación: Detenido, Iniciar y detener con el host

Valor sugerido de línea base: Detenido, Iniciar y detener manualmente

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VMHostService -VMHost $ESXi | Where-Object {$_.Key -eq 'sfcbd-watchdog' -and
$_.Running -eq 'True'}
```

```
Get-VMHostService -VMHost $ESXi | Where-Object {$_.Key -eq 'sfcbd-watchdog' -and $_.Policy
-eq 'On'}
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHostService -VMHost $ESXi | where {$_.Key -eq 'sfcbd-watchdog'} | Set-VMHostService
-Policy Off
Get-VMHostService -VMHost $ESXi | where {$_.Key -eq 'sfcbd-watchdog'} | Stop-VMHostService
```

Config.HostAgent.log.level

Establece el nivel informativo de registro.

Al configurar el nivel de registro, asegúrese de que haya suficiente información en los registros de auditoría para realizar diagnósticos y análisis forenses.

Valores

Valor predeterminado de instalación: información

Valor sugerido de línea base: información

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Los registros consumen espacio de almacenamiento adicional.

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Config.HostAgent.log.level
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Config.HostAgent.log.level | Set-
AdvancedSetting -Value info
```

Syslog.global.logLevel

Registra suficiente información de los eventos.

Sin suficientes datos de registro, los indicadores críticos de compromiso pueden pasar inadvertidos, lo que lleva a una mayor vulnerabilidad y posible incapacidad de responder de forma eficaz a los incidentes de ciberseguridad.

Valores

Valor predeterminado de instalación: error

Valor sugerido de línea base: información

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Los registros consumen espacio de almacenamiento adicional.

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Syslog.global.logLevel
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Syslog.global.logLevel | Set-AdvancedSetting
-Value info
```

Config.HostAgent.plugins.solo.enableMob

Desactiva el explorador de objetos administrados (Managed Object Browser, MOB).

Los servicios que no están en uso y que no son esenciales para las operaciones deben desactivarse.

Valores

Valor predeterminado de instalación: False

Valor sugerido de línea base: False

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Config.HostAgent.plugins.solo.enableMob
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Config.HostAgent.plugins.solo.enableMob | Set-
AdvancedSetting -Value False
```

Net.BlockGuestBPDU

Bloquea las transmisiones de la unidad de datos de protocolo de puente (BPDU) del sistema operativo invitado.

Las BPDU se utilizan para transmitir información del protocolo de árbol de expansión (STP) y detectar bucles de red. BPDU Guard y Portfast se activan normalmente en el conmutador físico conectado directamente al host ESXi para reducir el retraso de convergencia del árbol de expansión.

Sin embargo, si se envía un paquete de la BPDU desde una máquina virtual en el host ESXi al conmutador físico configurado, puede provocar un bloqueo en cascada de todas las interfaces de enlace ascendente del host ESXi. Para evitar este tipo de bloqueo, puede activar el filtro de la BPDU en el host ESXi para descartar cualquier paquete de la BPDU que se envíe al conmutador físico.

Los conmutadores virtuales estándar y distribuidos no admiten STP y no generan BPDU.

Valores

Valor predeterminado de instalación: 1

Valor sugerido de línea base: 1

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Algunas cargas de trabajo orientadas a redes pueden generar paquetes de BPDU de forma legítima. Compruebe que no haya paquetes de BPDU legítimos generados por las máquinas virtuales en el host ESXi antes de habilitar el filtro de BPDU. Si el filtro de BPDU está activado en esta situación, la habilitación de Rechazar transmisiones falsificadas en el grupo de puertos del conmutador virtual agrega protección contra bucles del árbol de expansión.

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Net.BlockGuestBPDU
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Net.BlockGuestBPDU | Set-AdvancedSetting
-Value 1
```

Net.DVFilterBindIpAddress

Restringe el uso de las API de red dvFilter.

Si no utiliza un producto como VMware NSX que utiliza la API de red dvFilter, no configure el host ESXi para enviar información de red a una dirección IP. Habilitar la API y hacer referencia a una dirección IP comprometida podría proporcionar acceso no autorizado a la red de otras máquinas virtuales en el host ESXi.

Si utiliza un producto que se basa en esta API, es importante comprobar que el host ESXi se haya configurado correctamente para garantizar una comunicación de red segura.

Valores

Valor predeterminado de instalación: ""

Valor sugerido de línea base: ""

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Net.DVFilterBindIpAddress
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Net.DVFilterBindIpAddress | Set-
AdvancedSetting -Value ""
```

UserVars.ESXiShellTimeOut

Establece un tiempo de espera para limitar el tiempo de ejecución de los servicios de ESXi Shell y SSH.

Esta configuración avanzada del sistema define una ventana de tiempo después de la cual los servicios ESXi Shell y SSH finalizan automáticamente.

Valores

Valor predeterminado de instalación: 0

Valor sugerido de línea base: 600

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting UserVars.ESXiShellTimeOut
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting UserVars.ESXiShellTimeOut | Set-
AdvancedSetting -Value 600
```

UserVars.SuppressShellWarning

Suprime la advertencia para las interfaces de soporte y solución de problemas.

El host ESXi no debe suprimir las advertencias de que ESXi Shell está activado.

Las advertencias que indican que SSH o ESXi Shell están activados pueden indicar que hay un ataque en curso. Es importante asegurarse de que SSH y ESXi Shell estén desactivados, y que esta configuración avanzada del sistema no esté activada.

Valores

Valor predeterminado de instalación: 0

Valor sugerido de línea base: 0

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting UserVars.SuppressShellWarning
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting UserVars.SuppressShellWarning | Set-
AdvancedSetting -Value 0
```

Configurar el daemon de Shell seguro ESXi para FIPS

El daemon de shell seguro (SSH) del host ESXi debe configurarse para utilizar solo cifrados validados por FIPS 140-2/140-3. Debe fortalecer y proteger los servicios del sistema cuando se activan.

Valores

Valor predeterminado de instalación: aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr

Valor sugerido de línea base: aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.ssh.server.config.list.invoke() | Where-Object {$_.Key -eq 'ciphers'} |
Select-Object -ExpandProperty Value
```

Ejemplo de corrección mediante un comando de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.system.ssh.server.config.set.CreateArgs()
$arguments.keyword = 'ciphers'
$arguments.value = 'aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-
ctr,aes128-ctr'
$ESXcli.system.ssh.server.config.set.Invoke($arguments)
```

Configurar el daemon SSH de ESXi para FIPS

El daemon SSH del host ESXi debe utilizar módulos criptográficos validados por FIPS 140-2/140-3.

OpenSSH en el host ESXi se envía con un módulo criptográfico validado por FIPS 140-2/140-3, activado de forma predeterminada. Por motivos de compatibilidad con versiones anteriores, puede desactivar este módulo. Audite y corrija si es necesario.

Valores

Valor predeterminado de instalación: True

Valor sugerido de línea base: true

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.security.fips140.ssh.get.Invoke()
```

Ejemplo de corrección mediante un comando de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.system.security.fips140.ssh.set.CreateArgs()
$arguments.enable = $true
$ESXcli.system.security.fips140.ssh.set.Invoke($arguments)
```

Configurar el daemon de Shell seguro ESXi para que no permita puertos de puerta de enlace

El daemon de Shell seguro (SSH) del host ESXi debe configurarse para que no permita puertos de puerta de enlace.

Debe fortalecer y proteger los servicios del sistema cuando se activan.

Valores

Valor predeterminado de instalación: No

Valor sugerido de línea base: No

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.ssh.server.config.list.invoke() | Where-Object {$_.Key -eq 'gatewayports'}
| Select-Object -ExpandProperty Value
```

Ejemplo de corrección mediante un comando de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.system.ssh.server.config.set.CreateArgs()
$arguments.keyword = 'gatewayports'
```

```
$arguments.value = 'no'
$ESXcli.system.ssh.server.config.set.Invoke($arguments)
```

Configurar el daemon de Shell seguro ESXi para que no utilice la autenticación basada en el host

El daemon de Shell seguro (SSH) del host ESXi no debe permitir la autenticación basada en el host.

Debe fortalecer y proteger los servicios del sistema cuando se activan.

Valores

Valor predeterminado de instalación: No

Valor sugerido de línea base: No

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.ssh.server.config.list.invoke() | Where-Object {$_.Key -eq
'hostbasedauthentication'} | Select-Object -ExpandProperty Value
```

Ejemplo de corrección mediante un comando de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.system.ssh.server.config.set.CreateArgs()
$arguments.keyword = 'hostbasedauthentication'
$arguments.value = 'no'
$ESXcli.system.ssh.server.config.set.Invoke($arguments)
```

Configurar el daemon de Shell seguro ESXi para establecer un recuento de tiempo de espera

El daemon de Shell seguro (SSH) del host ESXi debe establecer un recuento de tiempo de espera para las sesiones inactivas.

Debe fortalecer y proteger los servicios del sistema cuando se activan. El recuento de tiempo de espera multiplicado por el intervalo de tiempo de espera de inactividad es el número total de segundos que la sesión puede estar inactiva hasta que se desconecte.

Valores

Valor predeterminado de instalación: 3

Valor sugerido de línea base: 3

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.ssh.server.config.list.invoke() | Where-Object {$_.Key -eq
'clientalivecountmax'} | Select-Object -ExpandProperty Value
```

Ejemplo de corrección mediante un comando de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.system.ssh.server.config.set.CreateArgs()
$arguments.keyword = 'clientalivecountmax'
$arguments.value = '3'
$ESXcli.system.ssh.server.config.set.Invoke($arguments)
```

Configurar el daemon de Shell seguro ESXi para establecer un intervalo de tiempo de espera

El daemon de Shell seguro (SSH) del host ESXi debe establecer un recuento de tiempo de espera para las sesiones inactivas.

Debe fortalecer y proteger los servicios del sistema cuando se activan. El recuento de tiempo de espera multiplicado por el intervalo de tiempo de espera de inactividad es el número total de segundos que la sesión puede estar inactiva hasta que se desconecte.

Valores

Valor predeterminado de instalación: 200

Valor sugerido de línea base: 200

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.ssh.server.config.list.invoke() | Where-Object {$_.Key -eq
'clientaliveinterval'} | Select-Object -ExpandProperty Value
```

Ejemplo de corrección mediante un comando de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.system.ssh.server.config.set.CreateArgs()
$arguments.keyword = 'clientaliveinterval'
$arguments.value = '200'
$ESXcli.system.ssh.server.config.set.Invoke($arguments)
```

Configurar el daemon de Shell seguro ESXi para que muestre un aviso de inicio de sesión

El daemon de shell seguro (SSH) del host ESXi debe mostrar el aviso de inicio de sesión del sistema antes de conceder acceso a este.

Debe fortalecer y proteger los servicios del sistema cuando se activan. También debe establecer la configuración de `Config.Etc.issue` para proporcionar texto a este aviso.

Valores

Valor predeterminado de instalación: `/etc/issue`

Valor sugerido de línea base: `/etc/issue`

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.ssh.server.config.list.invoke() | Where-Object {$_.Key -eq 'banner'} |
Select-Object -ExpandProperty Value
```

Ejemplo de corrección mediante un comando de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.system.ssh.server.config.set.CreateArgs()
$arguments.keyword = 'banner'
```

```
$arguments.value = '/etc/issue'
$ESXcli.system.ssh.server.config.set.Invoke($arguments)
```

Configurar el daemon de Shell seguro ESXi para ignorar los archivos .rhosts

El daemon de Shell seguro (SSH) del host ESXi debe ignorar los archivos `.rhosts`.

Debe fortalecer y proteger los servicios del sistema cuando se activan.

Valores

Valor predeterminado de instalación: Sí

Valor sugerido de línea base: Sí

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.ssh.server.config.list.invoke() | Where-Object {$_.Key -eq 'ignorerhosts'}
| Select-Object -ExpandProperty Value
```

Ejemplo de corrección mediante un comando de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.system.ssh.server.config.set.CreateArgs()
$arguments.keyword = 'ignorerhosts'
$arguments.value = 'yes'
$ESXcli.system.ssh.server.config.set.Invoke($arguments)
```

Configurar el daemon de Shell seguro ESXi para desactivar el reenvío local de transmisión

El daemon de Shell seguro (SSH) del host ESXi debe desactivar el reenvío local de transmisión.

Debe fortalecer y proteger los servicios del sistema cuando se activan.

Valores

Valor predeterminado de instalación: No

Valor sugerido de línea base: No

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.ssh.server.config.list.invoke() | Where-Object {$_.Key -eq
'allowstreamlocalforwarding'} | Select-Object -ExpandProperty Value
```

Ejemplo de corrección mediante un comando de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.system.ssh.server.config.set.CreateArgs()
$arguments.keyword = 'allowstreamlocalforwarding'
$arguments.value = 'no'
$ESXcli.system.ssh.server.config.set.Invoke($arguments)
```

Configurar el daemon de Shell seguro ESXi para desactivar el reenvío de TCP

El daemon de shell seguro (SSH) del host ESXi debe desactivar el reenvío de TCP.

Debe fortalecer y proteger los servicios del sistema cuando se activan.

Valores

Valor predeterminado de instalación: No

Valor sugerido de línea base: No

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.ssh.server.config.list.invoke() | Where-Object {$_.Key -eq
'allowtcpforwarding'} | Select-Object -ExpandProperty Value
```

Ejemplo de corrección mediante un comando de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.system.ssh.server.config.set.CreateArgs()
$arguments.keyword = 'allowtcpforwarding'
$arguments.value = 'no'
$ESXcli.system.ssh.server.config.set.Invoke($arguments)
```

Configurar el daemon de Shell seguro ESXi para que no permita túneles

El daemon de Shell seguro (SSH) del host ESXi no debe permitir túneles.

Debe fortalecer y proteger los servicios del sistema cuando se activan.

Valores

Valor predeterminado de instalación: No

Valor sugerido de línea base: No

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.ssh.server.config.list.invoke() | Where-Object {$_.Key -eq 'permittunnel'}
| Select-Object -ExpandProperty Value
```

Ejemplo de corrección mediante un comando de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.system.ssh.server.config.set.CreateArgs()
$arguments.keyword = 'permittunnel'
$arguments.value = 'no'
$ESXcli.system.ssh.server.config.set.Invoke($arguments)
```

Configurar el daemon de Shell seguro ESXi para que no permita la configuración del entorno del usuario

El daemon de Shell seguro (SSH) del host ESXi no debe permitir la configuración del entorno del usuario.

Debe fortalecer y proteger los servicios del sistema cuando se activan.

Valores

Valor predeterminado de instalación: No

Valor sugerido de línea base: No

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.ssh.server.config.list.invoke() | Where-Object {$_.Key -eq
'permituserenvironment'} | Select-Object -ExpandProperty Value
```

Ejemplo de corrección mediante un comando de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.system.ssh.server.config.set.CreateArgs()
$arguments.keyword = 'permituserenvironment'
$arguments.value = 'no'
$ESXcli.system.ssh.server.config.set.Invoke($arguments)
```

Desactivar el servicio del protocolo de ubicación de servicios

Desactive el servicio del protocolo de ubicación de servicios (SLP) si no lo está utilizando.

Valores

Valor predeterminado de instalación: Detenido, Iniciar y detener manualmente

Valor sugerido de línea base: Detenido, Iniciar y detener manualmente

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VMHostService -VMHost $ESXi | Where-Object {$_.Key -eq 'slpd' -and $_.Running -eq
'True'}
Get-VMHostService -VMHost $ESXi | Where-Object {$_.Key -eq 'slpd' -and $_.Policy -eq 'On'}
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHostService -VMHost $ESXi | where {$_.Key -eq 'slpd'} | Set-VMHostService -Policy Off
Get-VMHostService -VMHost $ESXi | where {$_.Key -eq 'slpd'} | Stop-VMHostService
```

Mem.ShareForceSalting

Restringe el uso compartido transparente de páginas a las máquinas virtuales que están configuradas con `sched.mem.pshare.salt`.

El uso compartido transparente de páginas (TPS) es un método para reducir el espacio de memoria de las máquinas virtuales. En condiciones altamente controladas, los atacantes pueden utilizar el TPS para obtener acceso no autorizado a los datos de las máquinas virtuales vecinas. Las máquinas virtuales que no tienen establecida la configuración de `sched.mem.pshare.salt` no pueden compartir memoria con otras máquinas virtuales. Los tamaños de página grandes, una optimización del rendimiento en el hipervisor en muchas CPU modernas, no son compatibles con TPS.

Valores

Valor predeterminado de instalación: 2

Valor sugerido de línea base: 2

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Mem.ShareForceSalting
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Mem.ShareForceSalting | Set-AdvancedSetting
-Value 2
```

UserVars.HostClientSessionTimeout

Establece un tiempo de espera para finalizar automáticamente las sesiones del cliente del host ESXi inactivas.

El host ESXi debe finalizar automáticamente las sesiones del cliente del host inactivas. Esta práctica mitiga los posibles riesgos de seguridad al garantizar que las sesiones sin supervisión, que los usuarios no autorizados o el software malicioso podrían aprovechar, no se dejen abiertas de forma indefinida.

Valores

Valor predeterminado de instalación: 900

Valor sugerido de línea base: 900

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting UserVars.HostClientSessionTimeout
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting UserVars.HostClientSessionTimeout | Set-
AdvancedSetting -Value 900
```

Net.BMCNetworkEnable

Desactiva las interfaces de red de administración de hardware virtual.

Las controladoras de administración de hardware suelen presentar NIC virtuales o USB al host ESXi. Se pueden utilizar como puertas traseras y deben desactivarse tanto en la configuración del hardware como en la configuración de ESXi.

Valores

Valor predeterminado de instalación: 1

Valor sugerido de línea base: 0

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Algunas soluciones administradas de terceros pueden requerir esta funcionalidad.

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Net.BMCNetworkEnable
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHost -Name $ESXi | Get-AdvancedSetting Net.BMCNetworkEnable | Set-AdvancedSetting
-Value 0
```

Activar la autenticación de CHAP bidireccional/mutua para el tráfico iSCSI

Establezca la autenticación del adaptador de almacenamiento iSCSI en "Usar CHAP bidireccional" y proporcione las credenciales.

El CHAP mutuo proporciona una capa adicional de protección, ya que requiere que tanto el iniciador (cliente) como el destino (servidor) verifiquen sus identidades entre sí, lo que garantiza que las entidades no autorizadas no intercepten ni alteren los datos transmitidos entre los dos.

Valores

Valor predeterminado de la instalación: no configurado

Valor sugerido de línea base: activado

Acción necesaria

Modifique el valor predeterminado de la instalación si utiliza esta función.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VMHost -Name $ESXi | Get-VMHostHba | Where {$_.Type -eq "Iscsi"} | Select VMHost,
Device, ChapType, @{N="CHAPName";E={$_.AuthenticationProperties.ChapName}}
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VMHost -Name $ESXi | Get-VMHostHba | Where {$_.Type -eq "Iscsi"} | Set-VMHostHba
parameters
```

Para obtener información sobre los parámetros, consulte *Referencia de ESXCLI*.

No almacenar claves de cifrado en hosts ESXi sin proteger el acceso físico

El host ESXi no debe almacenar claves de cifrado en el propio host ESXi sin proteger el acceso físico al host.

La persistencia de claves es un mecanismo que utiliza un módulo de plataforma de confianza (TPM) local para almacenar claves del proveedor de claves estándar, que generalmente solo se encuentran en un sistema de administración de claves (KMS) externo. Si bien esta configuración puede mejorar la administración de dependencias, el uso de la persistencia de claves cambia los riesgos de cifrado. Si un atacante roba el host, tiene acceso a las claves de cifrado de los datos de ese host, lo que omite los controles de acceso del KMS externo. Por lo tanto, utilice la persistencia de claves solo cuando pueda garantizar la seguridad física de los hosts. Si los hosts físicos no son seguros y un atacante puede robar el host, el atacante también tiene los medios para acceder y utilizar cargas de trabajo cifradas.

La persistencia de claves y vSphere Native Key Provider a menudo se mezclan debido a que ambos almacenan datos de cifrado en los hosts. Sin embargo, vSphere Native Key Provider no utiliza la persistencia de claves, por lo que desactivar la persistencia de claves no lo afectará. Al igual que la persistencia de claves, vSphere Native Key Provider también requiere de una consideración cuidadosa de la seguridad física. Consulte Referencia de controles de seguridad para diseño del sistema de vSphere.

Valores

Valor predeterminado de instalación: False

Valor sugerido de línea base: False

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

El comportamiento deseado es el predeterminado. Cambiar el valor predeterminado puede afectar negativamente la confidencialidad en entornos donde es posible el acceso físico por parte de los atacantes.

Evaluación mediante comandos de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$ESXcli.system.security.keypersistence.get.invoke() | Select-Object -ExpandProperty Enabled
```

Ejemplo de corrección mediante un comando de PowerCLI

```
$ESXcli = Get-EsxCli -VMHost $ESXi -V2
$arguments = $ESXcli.system.security.keypersistence.disable.CreateArgs()
$arguments.removeallstoredkeys = $true
$ESXcli.system.security.keypersistence.disable.Invoke($arguments)
```

Referencia de controles de seguridad de vCenter Server

Estos controles de seguridad proporcionan un conjunto de líneas base de prácticas recomendadas de seguridad de vCenter Server. Están estructurados de manera tal que se explican los beneficios y las compensaciones de la implementación del control. Para realizar cambios, puede utilizar el vSphere Client, PowerCLI o la interfaz de administración de vCenter Server, según el control.

PowerCLI y variables utilizadas

Algunos de los ejemplos de PowerCLI utilizados aquí requieren que el módulo VMware.vSphere.SsoAdmin esté instalado.

Los comandos de PowerCLI de esta sección utilizan las siguientes variables:

- $VC="*vcenter_server_name*"
- $VDS="*vsphere_distributed_switch_name*"
- $VDPG="*vsphere_distributed_port_group*"

Establecer el tiempo de espera de inactividad de vSphere Client

El vCenter Server debe finalizar las sesiones del vSphere Client después de 15 minutos de inactividad.

Las sesiones del vSphere Client inactivas pueden dejarse abiertas de forma indefinida si un usuario olvida cerrar sesión, lo que aumenta el riesgo de un acceso privilegiado no autorizado.

Valores

Valor predeterminado de instalación: 120 minutos

Valor sugerido de línea base: 15 minutos

Acción recomendada

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

N/D (no hay API pública disponible)

Ejemplo de corrección mediante un comando de PowerCLI

N/D (no hay API pública disponible)

Establecer la ubicación en vSphere Client

Administración > Configuración del cliente > Tiempo de espera de sesión

Establecer el intervalo de intentos de inicio de sesión fallidos

El vCenter Server debe establecer el intervalo para contar los intentos de inicio de sesión fallidos en al menos 15 minutos.

Al limitar el número de intentos de inicio de sesión fallidos, se reduce el acceso no autorizado mediante la búsqueda de contraseñas de usuario, también conocida como "fuerza bruta".

Valores

Valor predeterminado de instalación: 180

Valor sugerido de línea base: 900

Acción recomendada

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-SsoLockoutPolicy | Select FailedAttemptIntervalSec
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-SsoLockoutPolicy | Set-SsoLockoutPolicy -FailedAttemptIntervalSec 900
```

Establecer la ubicación en vSphere Client

Administración > Single Sign On > Configuración > Cuentas locales > Directiva de bloqueo

Configurar el número máximo de intentos de la directiva de bloqueo de SSO de vSphere

El vCenter Server debe bloquear una cuenta después de un número determinado de intentos de inicio de sesión fallidos.

Los inicios de sesión fallidos repetidos de una cuenta pueden indicar problemas de seguridad. Para limitar los intentos de fuerza bruta, bloquee la cuenta después de un umbral determinado, estableciendo un equilibrio entre evitar los reintentos automáticos de conexión y los posibles ataques de denegación de servicio.

Valores

Valor predeterminado de instalación: 5

Valor sugerido de línea base: 5

Acción recomendada

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-SsoLockoutPolicy | Select MaxFailedAttempts
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-SsoLockoutPolicy | Set-SsoLockoutPolicy -MaxFailedAttempts 5
```

Establecer la ubicación en vSphere Client

Administración > Single Sign On > Configuración > Cuentas locales > Directiva de bloqueo

Configurar el tiempo de desbloqueo de la directiva de bloqueo de SSO de vSphere

El vCenter Server debe desbloquear las cuentas después de un período de tiempo de espera especificado.

Los inicios de sesión fallidos repetidos pueden sugerir amenazas de seguridad. Las cuentas de vCenter Server no deben desbloquearse automáticamente cuando se han bloqueado debido a varios errores de inicio de sesión. Asegúrese de que dispone de los datos de administrator@vsphere.local y de que son válidos.

Valores

Valor predeterminado de instalación: 300

Valor sugerido de línea base: 0

Acción recomendada

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Existe la oportunidad de denegación de servicio cuando las cuentas no se desbloquean automáticamente.

Evaluación mediante comandos de PowerCLI

```
Get-SsoLockoutPolicy | Select AutoUnlockIntervalSec
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-SsoLockoutPolicy | Set-SsoLockoutPolicy -AutoUnlockIntervalSec 0
```

Establecer la ubicación en vSphere Client

Administración > Single Sign On > Configuración > Cuentas locales > Directiva de bloqueo

Exigir complejidad de la contraseña

El vCenter Server debe exigir la complejidad de la contraseña.

Las prácticas recomendadas modernas para contraseñas (consulte la sección 5.1.1.2 de NIST 800-63B, entre otras instrucciones) indican que, con una entropía de contraseña adecuada, la seguridad no mejora al exigir arbitrariamente a los usuarios que cambien sus contraseñas a intervalos determinados. Muchas herramientas de seguridad automatizadas y algunos marcos de cumplimiento normativo no reflejan esta orientación y podrían pasar por alto esta recomendación.

Las reglas de seguridad y complejidad de las contraseñas se aplican a las cuentas creadas en vSphere SSO, incluido administrator@vsphere.local (o, si especificó un dominio diferente durante la instalación, administrator@*mydomain*). Estas reglas no se aplican a los usuarios de Active Directory cuando vCenter Server está unido a un dominio, ya que AD aplica esas directivas de contraseñas.

Valores

Valor predeterminado de instalación:

Longitud máxima: 20

Longitud mínima: 8

Al menos 1 especial

Al menos 2 alfabéticos

Al menos 1 en mayúscula

Al menos 1 en minúscula

Al menos 1 numérico

3 adyacentes idénticos

Valor sugerido de línea base:

Longitud máxima: 64

Longitud mínima: 15

Al menos 1 especial

Al menos 2 alfabéticos

Al menos 1 en mayúscula

Al menos 1 en minúscula

Al menos 1 numérico

3 adyacentes idénticos

Acción recomendada

Modifique los valores predeterminados de instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Es posible que otros productos y servicios dentro del ecosistema de VMware no esperen cambios en los requisitos de complejidad de las contraseñas y se produzca un error en la instalación.

Evaluación mediante comandos de PowerCLI

```
Get-SsoPasswordPolicy
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-SsoPasswordPolicy | Set-SsoPasswordPolicy -MinLength 15 -MaxLength 64 -MinNumericCount
1 -MinSpecialCharCount 1 -MinAlphabeticCount 2 -MinUppercaseCount 1 -MinLowercaseCount 1
-MaxIdenticalAdjacentCharacters 3
```

Establecer la ubicación en vSphere Client

Administración > Single Sign On > Configuración > Cuentas locales > Directiva de contraseña

Configurar el número máximo de días entre cambios de contraseña

El vCenter Server debe configurarse con una antigüedad máxima de contraseña adecuada.

Las prácticas recomendadas modernas para contraseñas (consulte la sección 5.1.1.2 de NIST 800-63B, entre otras instrucciones) indican que, con una entropía de contraseña adecuada, la seguridad no mejora al exigir arbitrariamente a los usuarios que cambien sus contraseñas a intervalos determinados. Muchas herramientas de seguridad automatizadas y algunos marcos de cumplimiento normativo no reflejan esta orientación y podrían pasar por alto esta recomendación.

Valores

Valor predeterminado de instalación: 90

Valor sugerido de línea base: 99999

Acción recomendada

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-SsoPasswordPolicy | Select PasswordLifetimeDays
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-SsoPasswordPolicy | Set-SsoPasswordPolicy -PasswordLifetimeDays 9999
```

Establecer la ubicación en vSphere Client

Administración > Single Sign On > Configuración > Cuentas locales > Directiva de contraseña

Restringir la reutilización de contraseñas

Configure la opción del historial de contraseñas para restringir la reutilización de contraseñas en el vCenter Server.

Las directrices de complejidad de las contraseñas en ocasiones hacen que los usuarios reutilicen contraseñas más antiguas. El ajuste del historial de contraseñas en el vCenter Server puede ayudar a evitar esta situación.

Valores

Valor predeterminado de instalación: 5

Valor sugerido de línea base: 5

Acción recomendada

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-SsoPasswordPolicy | Select ProhibitedPreviousPasswordsCount
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-SsoPasswordPolicy | Set-SsoPasswordPolicy -ProhibitedPreviousPasswordsCount 5
```

Establecer la ubicación en vSphere Client

Administración > Single Sign On > Configuración > Cuentas locales > Directiva de contraseña

Configurar el texto del banner de inicio de sesión para el acceso SSH

Configure el texto del banner de inicio de sesión del vCenter Server para el acceso mediante SSH.

vCenter Server permite mostrar un mensaje de inicio de sesión que disuade a los intrusos y comunica las obligaciones a los usuarios autorizados. Esta configuración establece el texto que se muestra cuando un cliente se conecta mediante SSH. El texto predeterminado filtra información a los atacantes sobre la configuración del sistema y debe cambiarse.

Valores

Valor predeterminado de instalación: VMware vCenter Server *version*

Tipo: vCenter Server con una instancia integrada de Platform Services Controller

Valor sugerido de línea base: consulte a los asesores legales de su organización para obtener un texto adecuado para su entorno.

Texto de ejemplo: Solo usuarios autorizados. El uso real o el intento de uso no autorizados de este sistema está prohibido y puede dar lugar a procedimientos o sanciones penales, civiles, de seguridad o administrativos. El uso de este sistema de información indica el consentimiento para la supervisión y el registro, sin previo aviso o permiso. Los usuarios no tienen expectativas de privacidad cuando usan este sistema. Cualquier información almacenada en este sistema, o en tránsito, u obtenida mediante la supervisión o registro, puede divulgarse a las autoridades policiales o utilizarse de acuerdo con la legislación federal, los estatutos estatales y la directiva de la organización. Si no es un usuario autorizado de este sistema, salga de él en este momento.

Acción recomendada

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-AdvancedSetting -Entity $VC -Name etc.issue
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-AdvancedSetting -Entity $VC -Name etc.issue | Set-AdvancedSetting -Value "Authorized
users only. Actual or attempted unauthorized use of this system is prohibited and may
result in criminal, civil, security, or administrative proceedings and/or penalties.
Use of this information system indicates consent to monitoring and recording, without
notice or permission. Users have no expectation of privacy in any use of this system.
Any information stored on, or transiting this system, or obtained by monitoring and/or
```

```
recording, may be disclosed to law enforcement and/or used in accordance with Federal law,
State statute, and organization policy. If you are not an authorized user of this system,
exit the system at this time."
```

Establecer la ubicación en vSphere Client

Administración > Single Sign On > Configuración > Mensaje de inicio de sesión

Establecer intervalo de retención de tareas y eventos

El vCenter Server debe tener la retención de tareas y eventos establecida en un intervalo adecuado.

vCenter Server conserva los datos de tareas y eventos, que caducan para ahorrar espacio de almacenamiento. La antigüedad se puede configurar. Esto solo afecta al almacenamiento local de los datos de eventos en el vCenter Server Appliance.

Valores

Valor predeterminado de instalación: 30

Valor sugerido de línea base: 30

Acción recomendada

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

N/D (no hay API pública disponible)

Ejemplo de corrección mediante un comando de PowerCLI

N/D (no hay API pública disponible)

Establecer la ubicación en vSphere Client

N/C

Activar el registro remoto

Active el registro remoto de eventos de vCenter Server.

El registro remoto en un host central mejora la seguridad de vCenter Server al almacenar los registros de forma segura. El registro remoto simplifica la supervisión en todos los hosts y admite análisis agregados para detectar ataques coordinados. El registro centralizado evita la manipulación y sirve como un registro de auditoría fiable a largo plazo. La opción `vpxd.event.syslog.enabled` activa el registro remoto.

Valores

Valor predeterminado de instalación: True

Valor sugerido de línea base: true

Acción recomendada

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-AdvancedSetting -Entity $VC -Name vpxd.event.syslog.enabled
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-AdvancedSetting -Entity $VC -Name vpxd.event.syslog.enabled | Set-AdvancedSetting
-Value true
```

Establecer la ubicación en vSphere Client

Seleccionar vCenter Server > Configurar > Configuración avanzada

Activar FIPS

El vCenter Server debe activar la criptografía validada por FIPS.

La criptografía FIPS realiza una serie de cambios en el sistema para eliminar cifrados más débiles. La activación de FIPS hace que se reinicie vCenter Server.

Valores

Valor predeterminado de instalación: False

Valor sugerido de línea base: true

Acción recomendada

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

La criptografía FIPS realiza una serie de cambios en el sistema para eliminar cifrados más débiles. Habilitar FIPS hace que se reinicie vCenter Server.

Evaluación mediante comandos de PowerCLI

```
Invoke-GetSystemGlobalFips
```

Ejemplo de corrección mediante un comando de PowerCLI

```
$spec = Initialize-SystemSecurityGlobalFipsUpdateSpec -Enabled $true
Invoke-SetSystemGlobalFips -SystemSecurityGlobalFipsUpdateSpec $spec
```

Establecer la ubicación en vSphere Client

Consulte Activar y desactivar FIPS en vCenter Server Appliance.

Configurar registros de auditoría

El vCenter Server debe producir registros de auditoría que contengan información para establecer qué tipo de eventos se produjeron.

Es importante asegurarse de que haya suficiente información en los registros de auditoría para fines de diagnóstico y análisis forense. La opción `config.log.level` configura los registros de auditoría.

Valores

Valor predeterminado de instalación: información

Valor sugerido de línea base: información

Acción recomendada

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-AdvancedSetting -Entity $VC -Name config.log.level
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-AdvancedSetting -Entity $VC -Name config.log.level | Set-AdvancedSetting -Value info
```

Establecer la ubicación en vSphere Client

Host de vCenter Server > Configurar > Configuración avanzada

Desactivar el aprendizaje de MAC

Todos los grupos de puertos del conmutador distribuido deben desactivar el aprendizaje de direcciones MAC, a menos que se utilice de forma intencional.

El aprendizaje de direcciones MAC permite que un conmutador distribuido proporcione conectividad de red a sistemas en los que se utiliza más de una dirección MAC en una vNIC. Esto puede resultar útil en casos especiales como la virtualización anidada (por ejemplo, para ejecutar ESXi dentro de ESXi). El aprendizaje de direcciones MAC también admite el desbordamiento de unidifusión desconocido. Normalmente, cuando un paquete recibido por un puerto tiene una dirección MAC de destino desconocido, el paquete se descarta. Cuando el desbordamiento de unidifusión desconocida está habilitado, el puerto envía el tráfico de unidifusión desconocida a cada puerto del conmutador que tenga habilitadas las opciones de desbordamiento de unidifusión desconocida y de aprendizaje de direcciones MAC. Esta propiedad está activada de forma predeterminada, pero solo si el aprendizaje de direcciones MAC está habilitado. Desactive el aprendizaje de direcciones MAC a menos que se esté utilizando de forma intencional para una carga de trabajo conocida que lo requiera.

Valores

Valor predeterminado de instalación: deshabilitado

Valor sugerido de línea base: deshabilitado

Acción recomendada

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Algunas cargas de trabajo utilizan legítimamente estas tácticas de red y se ven afectadas negativamente por los valores predeterminados y el estado deseado.

Evaluación mediante comandos de PowerCLI

```
(Get-VDPortgroup -Name
$VDPG).ExtensionData.Config.DefaultPortConfig.MacManagementPolicy.MacLearningPolicy |
Select-Object -ExpandProperty Enabled
```

Ejemplo de corrección mediante un comando de PowerCLI

```
$VDPGview = Get-VDPortgroup -Name $VDPG | Get-View
$ConfigSpec = New-Object VMware.Vim.DVPortgroupConfigSpec
$ConfigSpec.DefaultPortConfig = New-Object VMware.Vim.VMwareDVSPortSetting
$ConfigSpec.DefaultPortConfig.MacManagementPolicy = New-Object
VMware.Vim.DVSMacManagementPolicy
$ConfigSpec.DefaultPortConfig.MacManagementPolicy.MacLearningPolicy = New-Object
VMware.Vim.DVSMacLearningPolicy
$ConfigSpec.DefaultPortConfig.MacManagementPolicy.MacLearningPolicy.Enabled = $false
```

```
$ConfigSpec.ConfigVersion = $VDPGview.Config.ConfigVersion
$VDPGview.ReconfigureDVPortgroup_Task($ConfigSpec)
```

Establecer la ubicación en vSphere Client

N/D. El aprendizaje de direcciones MAC se puede habilitar en un grupo de puertos virtuales distribuidos mediante vSphere API. Consulte *Referencia de vSphere Web Services API* para obtener más información.

Configurar los detalles del banner del mensaje de inicio de sesión

Configure los detalles del banner de inicio de sesión de vCenter Server para el vSphere Client.

vCenter Server permite mostrar un mensaje de inicio de sesión. Los usos del mensaje de inicio de sesión incluyen informar a los intrusos que sus actividades son ilegales, y transmitir a los usuarios autorizados las expectativas y las obligaciones que deben cumplir y aceptar al utilizar el sistema. Esta configuración establece el texto detallado del mensaje de la página de inicio de sesión del vSphere Client.

Valores

Valor predeterminado de la instalación: no configurado

Valor sugerido de línea base: consulte a los asesores legales de su organización para obtener un texto adecuado para su entorno.

Texto de ejemplo: Solo usuarios autorizados. El uso real o el intento de uso no autorizados de este sistema está prohibido y puede dar lugar a procedimientos o sanciones penales, civiles, de seguridad o administrativos. El uso de este sistema de información indica el consentimiento para la supervisión y el registro, sin previo aviso o permiso. Los usuarios no tienen expectativas de privacidad cuando usan este sistema. Cualquier información almacenada en este sistema, o en tránsito, u obtenida mediante la supervisión o registro, puede divulgarse a las autoridades policiales o utilizarse de acuerdo con la legislación federal, los estatutos estatales y la directiva de la organización. Si no es un usuario autorizado de este sistema, salga de él en este momento.

Acción recomendada

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

N/D (no hay API pública disponible)

Puede configurar el mensaje de inicio de sesión ejecutando el siguiente comando en un shell de dispositivo:

```
/opt/vmware/bin/sso-config.sh -set_login_banner -title login_banner_title logonBannerFile
```

Recuerde volver a desactivar el shell cuando haya terminado.

Ejemplo de corrección mediante un comando de PowerCLI

N/D (no hay API pública disponible)

Puede configurar el mensaje de inicio de sesión ejecutando el siguiente comando en un shell de dispositivo:

```
/opt/vmware/bin/sso-config.sh -set_login_banner -title login_banner_title logonBannerFile
```

Recuerde volver a desactivar el shell cuando haya terminado.

Establecer la ubicación en vSphere Client

Administración > Single Sign On > Configuración > Mensaje de inicio de sesión > Editar

Activar el banner de inicio de sesión

Active el banner de inicio de sesión de vCenter Server para el vSphere Client.

vCenter Server permite mostrar un mensaje de inicio de sesión. Los usos del mensaje de inicio de sesión incluyen informar a los intrusos que sus actividades son ilegales, y transmitir a los usuarios autorizados las expectativas y las obligaciones que deben cumplir y aceptar al utilizar el sistema. Esta configuración activa la visualización del mensaje en la página de inicio de sesión de vSphere Client.

Valores

Valor predeterminado de instalación: False

Valor sugerido de línea base: true

Acción recomendada

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

N/D (no hay API pública disponible)

Puede configurar el mensaje de inicio de sesión ejecutando el siguiente comando en un shell de dispositivo:

```
/opt/vmware/bin/sso-config.sh -set_logon_banner -title logon_banner_title logonBannerFile
```

Recuerde volver a desactivar el shell cuando haya terminado.

Ejemplo de corrección mediante un comando de PowerCLI

N/D (no hay API pública disponible)

Puede configurar el mensaje de inicio de sesión ejecutando el siguiente comando en un shell de dispositivo:

```
/opt/vmware/bin/sso-config.sh -set_logon_banner -title logon_banner_title logonBannerFile
```

Recuerde volver a desactivar el shell cuando haya terminado.

Establecer la ubicación en vSphere Client

Administración > Single Sign On > Configuración > Mensaje de inicio de sesión > Editar

Configurar el texto del banner de inicio de sesión

Configure el texto del banner de inicio de sesión en vCenter Server para el vSphere Client.

vCenter Server permite mostrar un mensaje de inicio de sesión. Los usos del mensaje de inicio de sesión incluyen informar a los intrusos que sus actividades son ilegales, y transmitir a los usuarios autorizados las expectativas y las obligaciones que deben cumplir y aceptar al utilizar el sistema. Esta configuración establece el texto que se muestra en la página de inicio de sesión del vSphere Client.

Valores

Valor predeterminado de la instalación: no configurado

Valor sugerido de línea base: consulte a los asesores legales de su organización para obtener un texto específico.

Texto de ejemplo: El uso de este sistema indica el conocimiento y consentimiento de las directivas organizativas que lo rigen.

Acción recomendada

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

N/D (no hay API pública disponible)

Puede configurar el mensaje de inicio de sesión ejecutando el siguiente comando en un shell de dispositivo:

```
/opt/vmware/bin/sso-config.sh -set_logon_banner -title logon_banner_title logonBannerFile
```

Recuerde volver a desactivar el shell cuando haya terminado.

Ejemplo de corrección mediante un comando de PowerCLI

N/D (no hay API pública disponible)

Puede configurar el mensaje de inicio de sesión ejecutando el siguiente comando en un shell de dispositivo:

```
/opt/vmware/bin/sso-config.sh -set_logon_banner -title logon_banner_title logonBannerFile
```

Recuerde volver a desactivar el shell cuando haya terminado.

Establecer la ubicación en vSphere Client

Administración > Single Sign On > Configuración > Mensaje de inicio de sesión > Editar

Autenticación y autorización independientes para administradores

El vCenter Server debe separar la autenticación y la autorización de los administradores.

Al combinar autenticación y autorización, como hacen servicios como Active Directory, se corre el riesgo de que se produzcan brechas en la infraestructura si se produce un ataque. Por lo tanto, para vCenter Server, asegúrese de segregar la autenticación y la autorización para los administradores. Considere la posibilidad de utilizar grupos de SSO locales para la autorización a fin de administrar mejor el riesgo cuando sea posible.

Valores

Valor predeterminado de la instalación: no configurado

Valor sugerido de línea base: no configurado

Acción recomendada

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

El aprovisionamiento de acceso a vCenter Server requería la interacción con SSO de vCenter Server. La automatización es posible con PowerCLI.

Evaluación mediante comandos de PowerCLI

N/D (no hay API pública disponible)

Ejemplo de corrección mediante un comando de PowerCLI

N/D (no hay API pública disponible)

Establecer la ubicación en vSphere Client

N/C

Configurar la directiva de transmisiones falsificadas en Rechazar

Establezca todos los conmutadores distribuidos y sus grupos de puertos para que rechacen las transmisiones falsificadas.

Una máquina virtual puede suplantar adaptadores de red cambiando direcciones MAC, lo que supone una amenaza para la seguridad. Al establecer la opción Transmisiones falsificadas en Rechazar en todos los conmutadores y grupos de puertos distribuidos, ESXi verifica las direcciones MAC e impide dicha suplantación.

Valores

Valor predeterminado de instalación: Rechazar

Valor sugerido de línea base: Rechazar

Acción recomendada

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Algunas cargas de trabajo utilizan estas tácticas de red de forma legítima y se ven afectadas negativamente por el ajuste predeterminado.

Evaluación mediante comandos de PowerCLI

```
Get-VDSwitch -Name $VDS | Get-VDSecurityPolicy
Get-VDPortgroup -Name $VDPG | Get-VDSecurityPolicy
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VDSwitch -Name $VDS | Get-VDSecurityPolicy | Set-VDSecurityPolicy -ForgedTransmits
$false
Get-VDPortgroup -Name $VDPG | Get-VDSecurityPolicy | Set-VDSecurityPolicy -ForgedTransmits
$false
```

Establecer la ubicación en vSphere Client

Consulte la documentación de *Redes de vSphere*.

Establecer la directiva de cambios de dirección MAC en Rechazar

Establezca la directiva de cambios de dirección MAC en Rechazar tanto en el conmutador estándar de vSphere como en sus grupos de puertos.

Permitir que las máquinas virtuales cambien las direcciones MAC supone un riesgo de seguridad, ya que permite la suplantación de adaptadores de red. El rechazo de los cambios de MAC en todos los conmutadores distribuidos y grupos de puertos lo impide, pero puede afectar a ciertas aplicaciones, como la agrupación en clústeres de Microsoft o las licencias que dependen de las direcciones MAC. Realice excepciones a esta guía de seguridad según sea necesario.

Valores

Valor predeterminado de instalación: Rechazar

Valor sugerido de línea base: Rechazar

Acción recomendada

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Algunas cargas de trabajo utilizan legítimamente estas tácticas de red y se ven afectadas negativamente por el ajuste Rechazar.

Evaluación mediante comandos de PowerCLI

```
Get-VDSwitch -Name $VDS | Get-VDSecurityPolicy
Get-VDPortgroup -Name $VDPG | Get-VDSecurityPolicy
```

Evaluación mediante comandos de PowerCLI

```
Get-VDSwitch -Name $VDS | Get-VDSecurityPolicy | Set-VDSecurityPolicy -MacChanges $false
Get-VDPortgroup -Name $VDPG | Get-VDSecurityPolicy | Set-VDSecurityPolicy -MacChanges
$false
```

Establecer la ubicación en vSphere Client

Consulte la documentación de *Redes de vSphere*.

Establecer la directiva de modo promiscuo en Rechazar

Establezca la directiva de modo promiscuo en Rechazar tanto en el conmutador estándar de vSphere como en sus grupos de puertos.

La activación del modo promiscuo en un grupo de puertos permite a todas las máquinas virtuales conectadas leer todos los paquetes de red, lo que supone un riesgo potencial de seguridad. Aunque a veces es necesario permitir el modo promiscuo para depurar o supervisar, se recomienda usar el ajuste predeterminado Rechazar. Realice excepciones para grupos de puertos específicos según sea necesario.

Valores

Valor predeterminado de instalación: Rechazar

Valor sugerido de línea base: Rechazar

Acción recomendada

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Algunas cargas de trabajo utilizan legítimamente estas tácticas de red y se ven afectadas de forma negativa por el ajuste Rechazar.

Evaluación mediante comandos de PowerCLI

```
Get-VDSwitch -Name $VDS | Get-VDSecurityPolicy
Get-VDPortgroup -Name $VDPG | Get-VDSecurityPolicy
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VDSwitch -Name $VDS | Get-VDSecurityPolicy | Set-VDSecurityPolicy -AllowPromiscuous
$false
Get-VDPortgroup -Name $VDPG | Get-VDSecurityPolicy | Set-VDSecurityPolicy
-AllowPromiscuous $false
```

Establecer la ubicación en vSphere Client

Consulte la documentación de *Redes de vSphere*.

Restablecer la configuración del puerto cuando se desconectan las máquinas virtuales

El vCenter Server debe restablecer la configuración del puerto cuando las máquinas virtuales se desconectan.

Cuando una máquina virtual se desconecta del puerto del conmutador virtual, es conveniente restablecer la configuración del puerto para que otra máquina virtual que se conecte tenga un puerto en un estado conocido.

Valores

Valor predeterminado de instalación: activado

Valor sugerido de línea base: activado

Acción recomendada

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
(Get-VDPortgroup -Name $VDPG).ExtensionData.Config.Policy | Select-Object -ExpandProperty
PortConfigResetAtDisconnect
```

Ejemplo de corrección mediante un comando de PowerCLI

```
$VDPGview = Get-VDPortgroup -Name $VDPG | Get-View
$ConfigSpec = New-Object VMware.Vim.DVPortgroupConfigSpec
$ConfigSpec.DefaultPortConfig = New-Object VMware.Vim.VMwareDVSPortSetting
```

```
$ConfigSpec.Policy = New-Object VMware.Vim.VMwareDVSPortgroupPolicy
$ConfigSpec.Policy.PortConfigResetAtDisconnect = $true
$ConfigSpec.ConfigVersion = $VDPGview.Config.ConfigVersion
$VDPGview.ReconfigureDVPortgroup_Task($ConfigSpec)
```

Establecer la ubicación en vSphere Client

Consulte la documentación de *Redes de vSphere*.

Desactivar los protocolos Cisco Discovery Protocol o Link Layer Discovery Protocol

Desactive la participación en el protocolo Cisco Discovery Protocol (CDP) o Link Layer Discovery Protocol (LLDP) en los conmutadores distribuidos, a menos que se utilice de forma intencional.

El conmutador virtual distribuido de vSphere puede participar en CDP o LLDP, y podría compartir en la red información confidencial sin cifrar, como direcciones IP y nombres de sistema. Por lo tanto, CDP y LLDP pueden ayudar a los atacantes a comprender o suplantar su entorno. No obstante, CDP y LLDP también son sumamente útiles para los casos de uso legítimos. Desactive CDP y LLDP a menos que se necesiten para la validación de la configuración o la solución de problemas.

Valores

Valor predeterminado de instalación: Escuchar

Valor sugerido de línea base: Ninguno

Acción recomendada

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
(Get-VDSwitch -Name $VDS).ExtensionData.config.LinkDiscoveryProtocolConfig | Select-Object
-ExpandProperty Operation
```

Ejemplo de corrección mediante un comando de PowerCLI

```
$VDview = Get-VDSwitch -Name $VDS | Get-View
$ConfigSpec = New-Object VMware.Vim.VMwareDVSConfigSpec
$ConfigSpec.LinkDiscoveryProtocolConfig = New-Object VMware.Vim.LinkDiscoveryProtocolConfig
$ConfigSpec.LinkDiscoveryProtocolConfig.Protocol = 'cdp'
$ConfigSpec.LinkDiscoveryProtocolConfig.Operation = 'none'
$ConfigSpec.ConfigVersion = $VDview.Config.ConfigVersion
$VDview.ReconfigureDvs_Task($ConfigSpec)
```

Establecer la ubicación en vSphere Client

Consulte la documentación de *Redes de vSphere*.

Asegurarse de que los recopiladores autorizados reciban tráfico de NetFlow

El vCenter Server debe asegurarse de que el tráfico de NetFlow se envíe a los recopiladores autorizados.

El vSphere Distributed Switch puede exportar datos de NetFlow sin cifrar, revelando detalles sobre la red virtual y los patrones de tráfico. Compruebe que el uso de NetFlow esté autorizado y configurado correctamente para evitar fugas de información.

Valores

Valor predeterminado de instalación: Escuchar

Valor sugerido de línea base: Ninguno

Acción recomendada

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
(Get-VDSwitch -Name $VDS).ExtensionData.config.IpfixConfig.CollectorIpAddress | Select-
Object -ExpandProperty CollectorIpAddress
(Get-VDPortgroup -Name $VDPG).ExtensionData.Config.DefaultPortConfig.IpfixEnabled | Select-
Object -ExpandProperty Value
```

Ejemplo de corrección mediante un comando de PowerCLI

```
$VDPGview = Get-VDPortgroup -Name $VDPG | Get-View
$ConfigSpec = New-Object VMware.Vim.DVPortgroupConfigSpec
$ConfigSpec.DefaultPortConfig = New-Object VMware.Vim.VMwareDVSPortSetting
$ConfigSpec.DefaultPortConfig.IpfixEnabled = New-Object VMware.Vim.BoolPolicy
$ConfigSpec.DefaultPortConfig.IpfixEnabled.Inherited = $false
$ConfigSpec.DefaultPortConfig.IpfixEnabled.Value = $false
$ConfigSpec.ConfigVersion = $VDPGview.Config.ConfigVersion
$VDPGview.ReconfigureDVPortgroup_Task($ConfigSpec)
```

Establecer la ubicación en vSphere Client

Consulte la documentación de *Redes de vSphere*.

Configurar la seguridad de puertos de la máquina virtual

El vCenter Server no debe anular los ajustes del grupo de puertos en el nivel de puerto en los conmutadores distribuidos, excepto para bloquear puertos.

Si bien es posible que se necesiten anulaciones de configuración en el nivel de puertos para configuraciones de máquinas virtuales únicas, asegúrese de supervisarlas para evitar el uso no autorizado. Las anulaciones no supervisadas podrían permitir un acceso más amplio si se explota una configuración de Distributed Switch menos segura.

Valores

Valor predeterminado de instalación:

Anulación de bloqueo de puertos: TRUE

Todas las demás anulaciones: FALSE

Valor sugerido de línea base:

Anulación de bloqueo de puertos: TRUE

Todas las demás anulaciones: FALSE

Acción recomendada

Audite el ajuste predeterminado de instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
(Get-VDPortgroup -Name $VDPG).ExtensionData.Config.Policy
```

Ejemplo de corrección mediante un comando de PowerCLI

```
$VDPGview = Get-VDPortgroup -Name $VDPG | Get-View
$ConfigSpec = New-Object VMware.Vim.DVPortgroupConfigSpec
$ConfigSpec.DefaultPortConfig = New-Object VMware.Vim.VMwareDVSPortSetting
$ConfigSpec.Policy = New-Object VMware.Vim.VMwareDVSPortgroupPolicy
$ConfigSpec.Policy.UplinkTeamingOverrideAllowed = $false
$ConfigSpec.Policy.BlockOverrideAllowed = $true
$ConfigSpec.Policy.LivePortMovingAllowed = $false
$ConfigSpec.Policy.VlanOverrideAllowed = $false
$ConfigSpec.Policy.SecurityPolicyOverrideAllowed = $false
$ConfigSpec.Policy.VendorConfigOverrideAllowed = $false
$ConfigSpec.Policy.ShapingOverrideAllowed = $false
$ConfigSpec.Policy.IpfixOverrideAllowed = $false
$ConfigSpec.Policy.TrafficFilterOverrideAllowed = $false
$ConfigSpec.ConfigVersion = $VDPGview.Config.ConfigVersion
$VDPGview.ReconfigureDVPortgroup_Task($ConfigSpec)
```

Establecer la ubicación en vSphere Client

Consulte la documentación de *Redes de vSphere*.

Quitar reflejo de puertos

El vCenter Server debe quitar las sesiones de reflejo de puertos no autorizadas en los conmutadores distribuidos.

El vSphere Distributed Switch puede replicar el tráfico entre puertos, lo que permite la observación de tráfico. Para mantener la seguridad, se deben eliminar todas las sesiones de reflejo de puertos no autorizadas en los conmutadores distribuidos.

Valores

Valor predeterminado de la instalación: no configurado

Valor sugerido de línea base: no configurado

Acción recomendada

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
(Get-VDSwitch -Name $VDS).ExtensionData.config.VspanSession
```

Ejemplo de corrección mediante un comando de PowerCLI

N/C

Establecer la ubicación en vSphere Client

Consulte la documentación de *Redes de vSphere*.

Restringir el etiquetado de invitado virtual

El vCenter Server debe restringir el uso del etiquetado de invitado virtual (Virtual Guest Tagging, VGT) en los conmutadores distribuidos.

Establecer un grupo de puertos en VLAN 4095 permite el etiquetado de invitado virtual (VGT), lo que requiere que la máquina virtual procese las etiquetas de VLAN. Active VGT solo para las máquinas virtuales que estén autorizadas y equipadas para administrar etiquetas de VLAN. El uso inadecuado puede provocar una denegación de servicio o una interacción de tráfico de VLAN no autorizada.

Valores

Valor predeterminado de la instalación: no configurado

Valor sugerido de línea base: no configurado

Acción recomendada

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VDPortgroup -Name $VDPG | Where {$_.ExtensionData.Config.Uplink -ne "True"} | Select
Name,VlanConfiguration
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VDPortgroup $VDPG | Set-VDVlanConfiguration -VlanId "New_VLAN#"
```

Establecer la ubicación en vSphere Client

Consulte la documentación de *Redes de vSphere*.

Comprobar el mantenimiento VMware en la versión del vCenter Server

Asegúrese de que la versión de vCenter Server no esté en el estado Fin de soporte general de VMware.

Valores

Valor predeterminado de instalación: N/D

Valor sugerido de línea base: N/D

Acción recomendada

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

N/C

Ejemplo de corrección mediante un comando de PowerCLI

N/C

Establecer la ubicación en la interfaz de administración del vCenter Server

Actualizar

Restringir el acceso a SSH

El servicio SSH del vCenter Server se debe desactivar.

vCenter Server Appliance se entrega como un dispositivo y está pensado para administrarse a través de la interfaz de administración de vCenter Server, el vSphere Client y las API. SSH es una herramienta de solución de problemas y soporte que se activará solo cuando sea necesario. High Availability de vCenter Server utiliza SSH para coordinar la replicación y la conmutación por error entre los nodos. El uso de esta función requiere que SSH permanezca activado.

Valores

Valor predeterminado de instalación: desactivado

Valor sugerido de línea base: desactivado

Acción recomendada

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

Nota Primero debe conectarse al host de vCenter Server mediante el cmdlet `Connect-CISServer`.

```
(Get-CisService -Name "com.vmware.appliance.access.ssh").get()
```

Ejemplo de corrección mediante un comando de PowerCLI

```
(Get-CisService -Name "com.vmware.appliance.access.ssh").set($false)
```

Establecer la ubicación en la interfaz de administración del vCenter Server

Acceso

Comprobar la caducidad de la contraseña del usuario raíz

La caducidad de la contraseña de la cuenta raíz del vCenter Server debe configurarse correctamente.

Las prácticas recomendadas modernas para contraseñas (NIST 800-63B Sección 5.1.1.2, entre otras instrucciones) indican que, con una entropía de contraseña adecuada, la seguridad no mejora al requerir arbitrariamente a los usuarios que cambien sus contraseñas a intervalos determinados. Muchas herramientas de seguridad automatizadas y algunos marcos de cumplimiento normativo no reflejan esta orientación y podrían pasar por alto esta recomendación.

Valores

Valor predeterminado de instalación: Sí

Valor sugerido de línea base: No

Acción recomendada

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Si no se restablece la contraseña antes de que caduque, se necesitarán procedimientos de recuperación.

Evaluación mediante comandos de PowerCLI

Nota Primero debe conectarse al host de vCenter Server mediante el cmdlet `Connect-CISServer`.

```
(Get-CisService -Name "com.vmware.appliance.local_accounts.policy").get()
```

Ejemplo de corrección mediante un comando de PowerCLI

```
(Get-CisService -Name "com.vmware.appliance.local_accounts.policy").set(@{max_days=9999;
min_days=1; warn_days=7})
```

Establecer la ubicación en la interfaz de administración del vCenter Server

Administración

Configurar la copia de seguridad y la recuperación basadas en archivos

Configure la copia de seguridad y la recuperación basadas en archivos para poder recuperar el vCenter Server Appliance y su configuración mediante el instalador de vCenter Server. Las copias de seguridad y la restauración son una parte importante de la protección de su entorno.

Valores

Valor predeterminado de la instalación: no configurado

Valor sugerido de línea base: configuradas

Acción recomendada

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

N/C

Ejemplo de corrección mediante un comando de PowerCLI

N/C

Establecer la ubicación en la interfaz de administración del vCenter Server

Copia de seguridad

Configurar el firewall para que solo permita el tráfico desde redes autorizadas

El vCenter Server Appliance debe configurar el firewall para que solo permita el tráfico desde redes autorizadas.

Asegúrese de que todo el tráfico de red entrante y saliente esté bloqueado a menos que se permita explícitamente, lo que reduce la superficie de ataque y ayuda a evitar el acceso no autorizado al sistema. El tráfico saliente (egreso) no se bloquea, ni tampoco las conexiones relacionadas o establecidas, por lo que vCenter Server Appliance aún puede comunicarse con los sistemas en los que inicia la conexión. Utilice firewalls perimetrales para restringir ese tipo de conexiones.

Valores

Valor predeterminado de instalación: conexiones permitidas desde cualquier dirección IP.

Valor sugerido de línea base: conexiones permitidas solo desde estaciones de trabajo de infraestructura y administración autorizadas.

Acción recomendada

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Pérdida de conectividad. Asegúrese de configurar una regla de permiso para sí mismo antes de configurar una regla de "denegar todo".

Evaluación mediante comandos de PowerCLI

N/C

Ejemplo de corrección mediante un comando de PowerCLI

N/C

Establecer la ubicación en la interfaz de administración del vCenter Server

Firewall

Configurar un servidor de registro remoto

Configure un servidor de registro remoto para el vCenter Server.

El registro remoto en un host central mejora la seguridad de vCenter Server al almacenar los registros de forma segura. El registro remoto simplifica la supervisión en todos los hosts y admite análisis agregados para detectar ataques coordinados. El registro centralizado evita la manipulación y sirve como un registro de auditoría fiable a largo plazo.

Valores

Valor predeterminado de la instalación: no configurado

Valor sugerido de línea base: servidor de registro específico del sitio

Acción recomendada

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

Nota Primero debe conectarse al host de vCenter Server mediante el cmdlet `Connect-CISServer`.

```
(Get-CisService -Name "com.vmware.appliance.logging.forwarding").get()
```

Ejemplo de corrección mediante un comando de PowerCLI

N/C

Establecer la ubicación en vSphere Client

N/C

Configurar la sincronización de hora

vCenter Server debe tener orígenes de sincronización de hora fiables.

El cifrado, el registro de auditoría, las operaciones del clúster, la respuesta ante incidentes y los análisis forenses dependen en gran medida de la sincronización de la hora. El protocolo de tiempo de red (NTP) debe tener al menos cuatro orígenes. Si debe elegir entre dos orígenes y un origen, es preferible uno solo.

Valores

Valor predeterminado de instalación: no definido

Valor sugerido de línea base: específico del sitio, o bien:

0.vmware.pool.ntp.org,

1.vmware.pool.ntp.org,

2.vmware.pool.ntp.org,

3.vmware.pool.ntp.org

Acción recomendada

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

Nota Primero debe conectarse al host de vCenter Server mediante el cmdlet `Connect-CISServer`.

```
(Get-CisService -Name ""com.vmware.appliance.timesync"").get()
(Get-CisService -Name ""com.vmware.appliance.ntp"").get()
```

Ejemplo de corrección mediante un comando de PowerCLI

```
(Get-CisService -Name ""com.vmware.appliance.timesync"").set(""NTP"")
(Get-CisService -Name
""com.vmware.appliance.ntp"").set(""0.vmware.pool.ntp.org,1.vmware.pool.ntp.org,2.vmware.po
ol.ntp.org,3.vmware.pool.ntp.org"")
```

Establecer la ubicación en vSphere Client

N/C

Instalar las actualizaciones de software

Asegúrese de que vCenter Server tenga instaladas todas las actualizaciones de software.

Al mantener las revisiones de vCenter Server actualizadas, se pueden mitigar las vulnerabilidades. Los atacantes pueden aprovechar las vulnerabilidades conocidas al intentar obtener acceso no autorizado o elevar privilegios.

Al aplicar las actualizaciones, actualice primero vCenter Server si hay alguna actualización disponible y, a continuación, continúe con la actualización de ESXi. Esta secuencia garantiza que la capa de administración se actualice antes de actualizar los hosts ESXi.

Valores

Valor predeterminado de instalación: N/D

Valor sugerido de línea base: N/D

Acción recomendada

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

N/C

Ejemplo de corrección mediante un comando de PowerCLI

N/C

Establecer la ubicación en vSphere Client

Consulte la documentación de *Administración del ciclo de vida de hosts y clústeres*.

Rotar la contraseña de vpxuser

El vCenter Server debe configurar la contraseña de vpxuser para que se rote en el intervalo adecuado.

La opción `VirtualCenter.VimPasswordExpirationInDays` configura el período de rotación. Asegúrese de que el vCenter Server esté rotando correctamente la contraseña que establece automáticamente en los hosts ESXi.

Valores

Valor predeterminado de instalación: 30

Valor sugerido de línea base: 30

Acción recomendada

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-AdvancedSetting -Entity $VC -Name VirtualCenter.VimPasswordExpirationInDays
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-AdvancedSetting -Entity $VC -Name VirtualCenter.VimPasswordExpirationInDays | Set-
AdvancedSetting -Value 30
```

Establecer la ubicación en vSphere Client

Seleccionar vCenter Server > Configurar > Configuración avanzada

Referencia de controles de seguridad de máquinas virtuales

Estos controles de seguridad proporcionan un conjunto de líneas base de prácticas recomendadas de seguridad para máquinas virtuales. Están estructurados de manera tal que

se explican los beneficios y las compensaciones de la implementación del control. Para cambiar la configuración avanzada del sistema, puede utilizar la instancia de PowerCLI proporcionada o vSphere Client (**Host > Configurar > Sistema > Configuración avanzada del sistema**).

Variable utilizada

Los comandos de PowerCLI de esta sección utilizan la siguiente variable:

- $VM = "*virtual_machine_name*"

mks.enable3d

Desactiva las funciones de gráficos 3D en máquinas virtuales que no las necesitan para reducir los vectores de ataque potenciales, lo que mejora la seguridad general del sistema.

Valores

Valor predeterminado de instalación: False

Valor sugerido de línea base: False

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VM -Name $VM | Get-AdvancedSetting mks.enable3d
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VM -Name $VM | Get-AdvancedSetting mks.enable3d | Set-AdvancedSetting -Value FALSE
```

ethernet*.filter*.name

Limita el acceso a las máquinas virtuales a través de la API de red "dvFilter".

Herramientas como NSX utilizan la interfaz dvFilter para filtrar e inspeccionar el tráfico de red. Es posible que otras herramientas también la utilicen. Asegúrese de que esas herramientas estén autorizadas.

Valores

Valor predeterminado de instalación: no presente

Valor sugerido de línea base: no presente

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Es posible que las herramientas de red legítimas, incluyendo NSX, requieran esta funcionalidad.

Evaluación mediante comandos de PowerCLI

```
Get-VM -Name $VM | Get-AdvancedSetting "ethernet*.filter*.name*"
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VM -Name $VM | Get-AdvancedSetting "ethernet*.filter*.name*" | Remove-AdvancedSetting
```

Evitar que las máquinas virtuales arranquen desde orígenes no autorizados

Las máquinas virtuales deben evitar el arranque desde orígenes no autorizados.

Puede producirse un acceso no autorizado a una máquina virtual cuando su volumen de arranque principal no está disponible y el firmware EFI busca orígenes de arranque alternativos, como el arranque de red. Esto se puede mitigar mediante controles de red, así como con los parámetros avanzados `bios.bootDeviceClasses`, `bios.bootOrder` y `bios.hddOrder`.

`bios.bootDeviceClasses` tiene el formato "allow:XXXX" o "deny:XXXX", donde XXXX es una lista de clases de arranque delimitada por comas. Las clases de arranque son: net (arranque PXE de red), USB (desde dispositivos USB conectados); pcmcia (tarjetas de expansión PCMCIA, no utilizadas actualmente); cd (desde dispositivos virtuales de CD/DVD conectados); HD (desde discos duros virtuales conectados); fd (desde dispositivos de disquete virtuales conectados); reservado (desde dispositivos desconocidos); efishell (en el shell de EFI); y all (todos), o any (cualquiera) (igual que "all").

El uso de permitir o denegar también establece implícitamente lo contrario. Por ejemplo:

- deny:all no permite ninguna clase de arranque
- deny:net no permite el arranque de red, pero permite el resto
- allow:hd solo permite el arranque hd y niega el resto
- allow:hd,cd permite el arranque del dispositivo desde hd y después desde cd, y niega el resto

Las máquinas virtuales nuevas podrían requerir el arranque desde CD/DVD. Algunos entornos dinámicos, como labs, podrían usar el arranque desde red. Configure esos entornos según corresponda y documente sus razones.

Valores

Valor predeterminado de instalación: allow:all

Valor sugerido de línea base: allow:hd (una vez instalado el sistema operativo invitado)

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

La máquina virtual ya no puede arrancar desde orígenes no especificados, lo que puede afectar negativamente a situaciones en las que se requieren medios de recuperación o arranque desde PXE. No obstante, el parámetro puede cambiarse fácilmente a escala mediante PowerCLI. Un enfoque alternativo consiste en especificar métodos denegando, como "deny:net".

Evaluación mediante comandos de PowerCLI

```
Get-VM -Name $VM | Get-AdvancedSetting bios.bootDeviceClasses
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VM -Name $VM | Get-AdvancedSetting bios.bootDeviceClasses | Set-AdvancedSetting -Value
"allow:hd"
```

RemoteDisplay.maxConnections

Limita la cantidad de conexiones de consola a una máquina virtual.

Limitar el uso compartido de la consola de la máquina virtual a un usuario evita que haya varios observadores, lo que mejora la seguridad. Sin embargo, esto podría crear inadvertidamente una vía potencial para la denegación de servicio.

Valores

Valor predeterminado de instalación: -1

Valor sugerido de línea base: 1

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Podría crear una condición de denegación de servicio donde la consola es inutilizable porque el único usuario está conectado, o persiste una sesión de consola desconectada. Otros

productos, como VMware Cloud Director, pueden requerir que establezca esta opción en un valor mayor.

Evaluación mediante comandos de PowerCLI

```
Get-VM -Name $VM | Get-AdvancedSetting RemoteDisplay.maxConnections
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VM -Name $VM | Get-AdvancedSetting RemoteDisplay.maxConnections | Set-AdvancedSetting
-Value 1
```

Limitar la funcionalidad de acceso directo de dispositivos PCI

Las máquinas virtuales deben limitar la funcionalidad de acceso directo del dispositivo PCI.

Las características de E/S de DirectPath permiten que las máquinas virtuales accedan directamente al hardware del sistema, lo que afecta a las herramientas de mitigación de riesgos, como vMotion, DRS y High Availability. Las funciones de E/S de DirectPath también ofrecen potencialmente a los atacantes acceso privilegiado al hardware. Asegúrese de que solo las máquinas virtuales necesarias tengan este privilegio, compensándolo con controles de seguridad del sistema operativo invitado.

Valores

Valor predeterminado de instalación: no presente

Valor sugerido de línea base: no presente

Acción necesaria

Auditoría

Impacto funcional potencial si se cambia el valor predeterminado

Los dispositivos de acceso directo, como las GPU, se verían afectados de forma negativa si se desconectan. Audite y documente la necesidad empresarial de estas máquinas virtuales.

Evaluación mediante comandos de PowerCLI

```
Get-VM -Name $VM | Get-PassthroughDevice
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VM -Name $VM | Get-PassthroughDevice | Remove-PassthroughDevice
```

Quitar dispositivos de hardware virtual de máquina virtual innecesarios

Las máquinas virtuales deben eliminar el hardware virtual innecesario.

Para reducir las posibles fuentes de ataque, elimine el hardware virtual innecesario de las máquinas virtuales. Los puertos poco utilizados, las unidades de CD/DVD temporales y el hardware introducido por las migraciones podrían ser vulnerables. Si se eliminan, disminuye el riesgo de introducción de software o de exfiltración de datos de un entorno protegido.

Valores

Valor predeterminado de instalación: configurado

Valor sugerido de línea base: no presente

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

La eliminación del dispositivo de CD-ROM puede afectar a la instalación y el mantenimiento de VMware Tools. La eliminación de las controladoras XHCI puede afectar a la conectividad de teclado y mouse de la consola en algunos sistemas operativos invitados.

Evaluación mediante comandos de PowerCLI

```
$VMview = Get-VM -Name $VM | Get-View
$UnnecessaryHardware
= "VirtualUSBController|VirtualUSBXHCIController|VirtualParallelPort|VirtualFloppy|
VirtualSerialPort|VirtualHdAudioCard|VirtualAHCIController|VirtualEnsoniq1371|VirtualCdrom"

$VMview.Config.Hardware.Device | Where-Object {$_.GetType().Name -match
$UnnecessaryHardware} | Foreach-Object {
    $devname = $_.GetType().Name
    Write-Host "$VM`: [WARNING] VM has a $devname device. Please evaluate and consider
removing." -ForegroundColor Yellow
}
```

Ejemplo de corrección mediante un comando de PowerCLI

N/C

Establecer la ubicación en vSphere Client

Máquina virtual > Editar configuración > Hardware virtual

tools.guestlib.enableHostInfo

Impide que las máquinas virtuales obtengan información del host acerca del hipervisor.

Evitar que las máquinas virtuales obtengan información del host acerca del hipervisor reduce el riesgo de ataques avanzados, ya que niega a los adversarios detalles cruciales sobre el host físico.

Valores

Valor predeterminado de instalación: False

Valor sugerido de línea base: Falso o no definido

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VM -Name $VM | Get-AdvancedSetting tools.guestlib.enableHostInfo
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VM -Name $VM | Get-AdvancedSetting tools.guestlib.enableHostInfo | Remove-
AdvancedSetting
```

Establecer la ubicación en vSphere Client

N/A. Este es un ajuste de archivo VMX.

Establecer cifrado para Fault Tolerance

Las máquinas virtuales deben requerir cifrado para Fault Tolerance.

Requerir cifrado para Fault Tolerance en las máquinas virtuales garantiza una transmisión de datos segura. Si bien el cifrado "oportunista" predeterminado probablemente da como resultado el cifrado debido a la compatibilidad omnipresente de AES-NI en el hardware compatible con vSphere, forzar cifrado "requerido" garantiza que no haya operaciones sin cifrar.

Valores

Valor predeterminado de instalación: ftEncryptionOpportunistic

Valor sugerido de línea base: ftEncryptionRequired

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
(Get-VM -Name $VM).ExtensionData.Config.FtEncryptionMode
```

Ejemplo de corrección mediante un comando de PowerCLI

```
$VMview = Get-VM -Name $VM | Get-View
$ConfigSpec = New-Object VMware.Vim.VirtualMachineConfigSpec
```

```
$ConfigSpec.FtEncryptionMode = New-object
VMware.Vim.VirtualMachineConfigSpecEncryptedFtModes
$ConfigSpec.FtEncryptionMode = "ftEncryptionRequired"
$VMview.ReconfigVM_Task($ConfigSpec)
```

Establecer la ubicación en vSphere Client

Máquina virtual > Editar ajustes > Opciones de máquina virtual > Cifrado

isolation.tools.copy.disable

Desactiva las operaciones de copia de la consola en las máquinas virtuales.

Desactivar las operaciones de copia de la consola en las máquinas virtuales impide la copia de datos entre la máquina virtual y el cliente local, independientemente de si el usuario accede a través de Web Console, VMRC u otro método.

Valores

Valor predeterminado de instalación: True

Valor sugerido de línea base: True o Undefined

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VM -Name $VM | Get-AdvancedSetting isolation.tools.copy.disable
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VM -Name $VM | Get-AdvancedSetting isolation.tools.copy.disable | Remove-
AdvancedSetting
```

isolation.tools.paste.disable

Desactiva las operaciones de pegado de la consola en las máquinas virtuales.

Al deshabilitar las operaciones de pegado de la consola en las máquinas virtuales, se bloquea la transferencia de datos del cliente local a la máquina virtual, independientemente de si el usuario utiliza la consola web, VMRC u otra consola.

Valores

Valor predeterminado de instalación: True

Valor sugerido de línea base: True o Undefined

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VM -Name $VM | Get-AdvancedSetting isolation.tools.paste.disable
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VM -Name $VM | Get-AdvancedSetting isolation.tools.paste.disable | Remove-
AdvancedSetting
```

isolation.tools.diskShrink.disable

Desactiva la reducción de discos virtuales en las máquinas virtuales.

Deshabilitar la reducción de discos virtuales en máquinas virtuales ayuda a evitar problemas de falta de disponibilidad de los discos. La capacidad de realizar esta operación suele estar limitada para los usuarios no administrativos en el entorno invitado.

Valores

Valor predeterminado de instalación: True

Valor sugerido de línea base: True o Undefined

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VM -Name $VM | Get-AdvancedSetting isolation.tools.diskShrink.disable
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VM -Name $VM | Get-AdvancedSetting isolation.tools.diskShrink.disable | Remove-
AdvancedSetting
```

isolation.tools.diskWiper.disable

Desactiva las operaciones de borrado de discos virtuales en las máquinas virtuales.

Deshabilitar el borrado de discos virtuales en las máquinas virtuales ayuda a evitar problemas de falta de disponibilidad de los discos. La capacidad de realizar esta operación suele estar limitada para los usuarios no administrativos en el entorno invitado.

Valores

Valor predeterminado de instalación: True

Valor sugerido de línea base: True o Undefined

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VM -Name $VM | Get-AdvancedSetting isolation.tools.diskWiper.disable
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VM -Name $VM | Get-AdvancedSetting isolation.tools.diskWiper.disable | Remove-
AdvancedSetting
```

isolation.device.connectable.disable

Evita que las máquinas virtuales eliminen, conecten y modifiquen dispositivos sin autorización.

Evitar las modificaciones de dispositivos no autorizadas en máquinas virtuales impide que los usuarios o procesos que no sean administrativos conecten o desconecten dispositivos o cambien su configuración. Esta medida limita el acceso no autorizado y la interrupción de las operaciones, lo que reduce los riesgos de denegación de servicio, así como algunas vías para exfiltrar datos.

Valores

Valor predeterminado de instalación: True

Valor sugerido de línea base: True o Undefined

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VM -Name $VM | Get-AdvancedSetting isolation.device.connectable.disable
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VM -Name $VM | Get-AdvancedSetting isolation.device.connectable.disable | Remove-
AdvancedSetting
```

isolation.tools.dnd.disable

Desactiva las operaciones de arrastrar y soltar en las consolas de máquinas virtuales.

La desactivación de las operaciones de arrastrar y soltar en la consola de una máquina virtual impide que los usuarios transfieran datos entre la máquina virtual y el cliente local, independientemente del tipo de consola, lo que mejora la seguridad de los datos.

Valores

Valor predeterminado de instalación: True

Valor sugerido de línea base: True o Undefined

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VM -Name $VM | Get-AdvancedSetting isolation.tools.dnd.disable
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VM -Name $VM | Get-AdvancedSetting isolation.tools.dnd.disable | Remove-AdvancedSetting
```

tools.setInfo.sizeLimit

Limita los mensajes informativos que se transmiten de la máquina virtual al archivo VMX.

La limitación de los mensajes informativos de la máquina virtual al archivo VMX evita que se supere el tamaño predeterminado de 1 MB. Esta opción evita posibles situaciones de denegación de servicio que podrían surgir si el almacén de datos se llena.

Valores

Valor predeterminado de instalación: 1048576

Valor sugerido de línea base: 1048576 o no definido

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VM -Name $VM | Get-AdvancedSetting tools.setInfo.sizeLimit
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VM -Name $VM | Get-AdvancedSetting tools.setInfo.sizeLimit | Remove-AdvancedSetting
```

Activar el registro

Las máquinas virtuales deben activar el registro de diagnóstico.

El registro de diagnóstico de las máquinas virtuales sirve de ayuda para los análisis forenses y la solución de problemas.

Valores

Valor predeterminado de instalación: True

Valor sugerido de línea base: true

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VM -Name $VM | Where {$_.ExtensionData.Config.Flags.EnableLogging -ne "True"}
```

Ejemplo de corrección mediante un comando de PowerCLI

```
$VMview = Get-VM -Name $VM | Get-View
$ConfigSpec = New-Object VMware.Vim.VirtualMachineConfigSpec
$ConfigSpec.Flags = New-Object VMware.Vim.VirtualMachineFlagInfo
$ConfigSpec.Flags.EnableLogging = $true
$VMview.ReconfigVM_Task($ConfigSpec)
```

log.keepOld

Limita la cantidad de registros de diagnóstico de máquinas virtuales retenidos.

Al restringir la cantidad de registros de diagnóstico retenidos, se evita llenar el almacén de datos sin comprometer la funcionalidad de diagnóstico.

Valores

Valor predeterminado de instalación: 10

Valor sugerido de línea base: 10 o no definido

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VM -Name $VM | Get-AdvancedSetting log.keepOld
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VM -Name $VM | Get-AdvancedSetting log.keepOld | Remove-AdvancedSetting
```

log.rotateSize

Limita el tamaño de los registros de diagnóstico de las máquinas virtuales.

Limitar el tamaño de los registros de diagnóstico en las máquinas virtuales evita un consumo de espacio excesivo, particularmente en máquinas virtuales de larga ejecución. El límite mínimo recomendado es de 2 MB.

Valores

Valor predeterminado de instalación: 2048000

Valor sugerido de línea base: 2048000 o no definido

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VM -Name $VM | Get-AdvancedSetting log.rotateSize
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VM -Name $VM | Get-AdvancedSetting log.rotateSize | Remove-AdvancedSetting
```

tools.guestlib.enableHostInfo

Desactiva la capacidad de enviar información del host a los invitados.

Al configurar una máquina virtual para obtener información detallada sobre el host físico, un atacante podría utilizar esta información para perpetrar futuros ataques contra el host. Dado que el valor predeterminado es el estado deseado, puede realizar una auditoría comprobando que esta opción no esté establecida o bien, si lo está, que está establecida en False.

Valores

Valor predeterminado de instalación: False

Valor sugerido de línea base: Falso o No definido

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

La imposibilidad de recuperar información de rendimiento sobre el host desde el sistema operativo invitado podría dificultar la solución de problemas.

Evaluación mediante comandos de PowerCLI

```
Get-VM -Name $VM | Get-AdvancedSetting tools.guestlib.enableHostInfo
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VM -Name $VM | Get-AdvancedSetting tools.guestlib.enableHostInfo | Remove-
AdvancedSetting
```

tools.guest.desktop.autolock

Bloquea la sesión de invitado de la máquina virtual cuando se desconecta la consola remota.

Bloquear las máquinas virtuales cuando se cierra la última conexión de la consola puede impedir el acceso no autorizado de atacantes que aprovechan las sesiones iniciadas de la consola.

Valores

Valor predeterminado de instalación: False

Valor sugerido de línea base: true

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VM -Name $VM | Get-AdvancedSetting tools.guest.desktop.autolock
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Get-VM -Name $VM | Get-AdvancedSetting tools.guest.desktop.autolock | Remove-
AdvancedSetting
```

Activar el cifrado para vMotion

Las máquinas virtuales deben requerir cifrado para vMotion.

Requerir cifrado para vMotion en las máquinas virtuales garantiza una transferencia de datos segura. El cifrado "oportunista" predeterminado probablemente da como resultado el cifrado debido a la compatibilidad generalizada de AES-NI en el hardware compatible con vSphere. No obstante, forzar el cifrado "obligatorio" evita las operaciones sin cifrar.

Valores

Valor predeterminado de instalación: Oportunista

Valor sugerido de línea base: Obligatorio

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
(Get-VM -Name $VM).ExtensionData.Config.MigrateEncryption
```

Ejemplo de corrección mediante un comando de PowerCLI

```
$VMview = Get-VM -Name $VM | Get-View
$ConfigSpec = New-Object VMware.Vim.VirtualMachineConfigSpec
$ConfigSpec.MigrateEncryption = New-Object
VMware.Vim.VirtualMachineConfigSpecEncryptedVMotionModes
```

```
$ConfigSpec.MigrateEncryption = "required"
$VMview.ReconfigVM_Task($ConfigSpec)
```

Controles de seguridad del sistema operativo invitado

Estos controles de seguridad proporcionan un conjunto de líneas base de prácticas recomendadas para el sistema operativo invitado. Están estructurados de manera tal que se explican los beneficios y las compensaciones de la implementación del control. Para realizar cambios en estos controles, utilice la PowerCLI proporcionada o vSphere Client.

Variable utilizada

Los comandos de PowerCLI de esta sección utilizan la siguiente variable:

- $VM = "*virtual_machine_name*"

Ruta de VMware Tools

La ruta de instalación predeterminada de VMware Tools es `C:\Program Files\VMware\VMware Tools`.

Configurar el arranque seguro del sistema operativo invitado

El sistema operativo invitado debe habilitar el arranque seguro.

El arranque seguro, compatible con todos los sistemas operativos invitados modernos, utiliza criptografía de clave pública para validar el firmware, el cargador de arranque, los controladores y el kernel del sistema operativo. Al evitar el arranque del sistema con validez de cadena de arranque incierta, el arranque seguro restringe el malware de forma eficaz.

Valores

Valor predeterminado de instalación: específico del sitio

Valor sugerido de línea base: true

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Habilitar el arranque seguro después de instalar un sistema operativo invitado puede implicar más pasos. Consulte la documentación del sistema operativo invitado para obtener instrucciones.

Evaluación mediante comandos de PowerCLI

```
(Get-VM -Name $VM).ExtensionData.Config.BootOptions.EfiSecureBootEnabled
```

Ejemplo de corrección mediante un comando de PowerCLI

```
$VMobj = (Get-VM -Name $VM)
$ConfigSpec = New-Object VMware.Vim.VirtualMachineConfigSpec
$bootOptions = New-Object VMware.Vim.VirtualMachineBootOptions
$bootOptions.EfiSecureBootEnabled = $true
$ConfigSpec.BootOptions = $bootOptions
$task = $VMobj.ExtensionData.ReconfigVM_Task($ConfigSpec)
```

Establecer la ubicación en vSphere Client

Máquina virtual > Editar configuración > Opciones de máquinas virtuales

Limitar el uso de transformaciones de MSI

El sistema operativo invitado debe limitar el uso de transformaciones de MSI al volver a configurar VMware Tools.

Las transformaciones de MSI permiten cambiar la base de datos de instalación en los sistemas operativos invitados de Microsoft Windows. Esto puede ser útil, pero también presenta la oportunidad de modificar el perfil de seguridad del sistema operativo invitado desde vSphere.

Valores

Valor predeterminado de instalación: False

Valor sugerido de línea base: False

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Los administradores deben utilizar otros métodos para actualizar y volver a configurar VMware Tools cuando sea necesario.

Evaluación mediante comandos de PowerCLI

```
VMwareToolboxCmd.exe config get autoupgrade allow-msi-transforms
```

Ejemplo de corrección mediante un comando de PowerCLI

```
VMwareToolboxCmd.exe config set autoupgrade allow-msi-transforms false
```

Establecer la ubicación en vSphere Client

N/C

Desactivar Appinfo

El sistema operativo invitado debe desactivar la recopilación de información de Appinfo, a menos que sea necesaria.

Appinfo es un método de detección de aplicaciones a través de VMware Tools. Si no utiliza esta herramienta, desactive el módulo para reducir la superficie de ataque.

Valores

Valor predeterminado de instalación: False

Valor sugerido de línea base: true

Acción necesaria

Modifique el valor predeterminado de instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Es posible que los productos y servicios dentro del ecosistema de VMware requieran esta funcionalidad.

Evaluación mediante comandos de PowerCLI

```
VMwareToolboxCmd.exe config get appinfo disabled
```

Ejemplo de corrección mediante un comando de PowerCLI

```
VMwareToolboxCmd.exe config set appinfo disabled true
```

Establecer la ubicación en vSphere Client

N/C

Desactivar ContainerInfo

El sistema operativo invitado debe desactivar ContainerInfo, a menos que sea necesario.

El complemento ContainerInfo de VMware Tools para Linux recopila la lista de contenedores en ejecución dentro de un sistema operativo invitado de Linux.

Valores

Valor predeterminado de instalación: 21600

Valor sugerido de línea base: 0

Acción necesaria

Modifique el valor predeterminado de instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Es posible que los productos y servicios dentro del ecosistema de VMware requieran esta funcionalidad.

Evaluación mediante comandos de PowerCLI

```
VMwareToolboxCmd.exe config get containerinfo poll-interval
```

Ejemplo de corrección mediante un comando de PowerCLI

```
VMwareToolboxCmd.exe config set containerinfo poll-interval 0
```

Establecer la ubicación en vSphere Client

N/C

Desactivar operaciones de invitado

Desactive las operaciones de invitado, a menos que sean necesarias.

Las operaciones de invitado son un conjunto de funciones que permiten la mayor parte de la interacción entre hosts e invitados. Desactivarlas permite reducir la superficie de ataque, pero también disminuye drásticamente la funcionalidad. Asegúrese de que el entorno no requiera estas funciones. No desactive las operaciones de invitado en las máquinas virtuales de la plantilla.

Para obtener una lista de las funciones, consulte la siguiente documentación:

https://vdc-download.vmware.com/vmwb-repository/dcr-public/fe08899f-1eec-4d8d-b3bc-a6664c168c2c/7fdf97a1-4c0d-4be0-9d43-2ceebbc174d9/doc/vim.vm.guest.GuestOperationsManager.html

Valores

Valor predeterminado de instalación: False

Valor sugerido de línea base: true

Acción necesaria

Modifique el valor predeterminado de instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Es posible que los productos y servicios dentro del ecosistema de VMware requieran esta funcionalidad.

Evaluación mediante comandos de PowerCLI

```
VMwareToolboxCmd.exe config get guestoperations disabled
```

Ejemplo de corrección mediante un comando de PowerCLI

```
VMwareToolboxCmd.exe config set guestoperations disabled true
```

Establecer la ubicación en vSphere Client

N/C

Evitar volver a personalizar el sistema operativo invitado

Debe evitar que el sistema operativo invitado de las máquinas virtuales implementadas y personalizadas se vuelva a personalizar.

El proceso de implementación de máquinas virtuales ofrece muchas opciones para que los administradores de vSphere personalicen las máquinas virtuales mediante scripts y la ejecución de comandos. Estos enfoques de personalización también pueden ser una vía para que un adversario obtenga acceso a los datos dentro de una máquina virtual, al clonarlos y volver a personalizarlos. Después de implementar una máquina virtual, evite que se vuelva a personalizar. Siempre puede revertir este cambio.

Valores

Valor predeterminado de instalación: True

Valor sugerido de línea base: False

Acción necesaria

Modifique el valor predeterminado de instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Una vez configuradas, las máquinas virtuales pueden personalizarse cuando se clonan. No realice este cambio en las máquinas virtuales de la plantilla.

Realizar este cambio puede afectar los procesos de recuperación ante desastres que cambian las direcciones IP, a través de VMware Site Recovery Manager o VMware Cloud Disaster Recovery. Para obtener más información consulte la siguiente documentación:

https://docs.vmware.com/es/VMware-Cloud-Disaster-Recovery/services/vmware-cloud-disaster-recovery/GUID-94202BE7-FEAF-4E35-8B55-15F6B3798309.html

Evaluación mediante comandos de PowerCLI

```
VMwareToolboxCmd.exe config get deployPkg enable-customization
```

Ejemplo de corrección mediante un comando de PowerCLI

```
VMwareToolboxCmd.exe config set deployPkg enable-customization false
```

Establecer la ubicación en vSphere Client

N/C

Desactivar las operaciones de actualización de GuestStore

El sistema operativo invitado debe desactivar las operaciones de actualización de GuestStore, a menos que sean necesarias.

La función GuestStore proporciona un mecanismo simple y flexible para distribuir contenido específico o personalizado de VMware desde un repositorio de GuestStore a varios invitados al mismo tiempo. Si no utiliza esta función, desactive el complemento para reducir la superficie de ataque.

Valores

Valor predeterminado de instalación: manual

Valor sugerido de línea base: desactivado

Acción necesaria

Modifique el valor predeterminado de instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Es posible que los productos y servicios dentro del ecosistema de VMware requieran esta funcionalidad.

Evaluación mediante comandos de PowerCLI

```
VMwareToolboxCmd.exe config get guestStoreupgrade policy
```

Ejemplo de corrección mediante un comando de PowerCLI

```
VMwareToolboxCmd.exe config set guestStoreupgrade policy off
```

Establecer la ubicación en vSphere Client

N/C

Desactivar la detección de servicios

El sistema operativo invitado debe desactivar la detección de servicios, a menos que sea necesaria.

El complemento de detección de servicios de VMware Tools se conecta a Aria Operations y proporciona datos adicionales a ese producto sobre los sistemas operativos invitados y las cargas de trabajo. Si no utiliza esta función, desactive el complemento para reducir la superficie de ataque.

Valores

Valor predeterminado de instalación: False

Valor sugerido de línea base: true

Acción necesaria

Modifique el valor predeterminado de instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Es posible que los productos y servicios dentro del ecosistema de VMware requieran esta funcionalidad.

Evaluación mediante comandos de PowerCLI

```
VMwareToolboxCmd.exe config get servicediscovery disabled
```

Ejemplo de corrección mediante un comando de PowerCLI

```
VMwareToolboxCmd.exe config set servicediscovery disabled true
```

Establecer la ubicación en vSphere Client

N/C

Activar el registro de VMware Tools

El sistema operativo invitado debe habilitar el registro de VMware Tools.

Asegúrese de que VMware Tools registre la información según corresponda. Consulte https://github.com/vmware/open-vm-tools/blob/master/open-vm-tools/tools.conf para ver ejemplos.

Valores

Valor predeterminado de instalación: True

Valor sugerido de línea base: true

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
VMwareToolboxCmd.exe config get logging log
```

Ejemplo de corrección mediante un comando de PowerCLI

```
VMwareToolboxCmd.exe config set logging log true
```

Establecer la ubicación en vSphere Client

N/C

Enviar registros de VMware Tools al servicio de registro del sistema

El sistema operativo invitado debe enviar registros de VMware Tools al servicio de registros del sistema.

De forma predeterminada, VMware Tools envía registros a un archivo en el disco. Configure los registros que se enviarán a syslog en los invitados de Linux y al servicio de eventos de Windows en invitados de Microsoft Windows para la administración y el archivado central.

Valores

Valor predeterminado de instalación: archivo

Valor sugerido de línea base: syslog

Acción necesaria

Modifique el valor predeterminado de instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Actualice los procesos que dependen de que estos archivos se encuentren en la ubicación predeterminada.

Evaluación mediante comandos de PowerCLI

```
VMwareToolboxCmd.exe config get logging vmsvc.handler
VMwareToolboxCmd.exe config get logging toolboxcmd.handler
VMwareToolboxCmd.exe config get logging vgauthsvc.handler
VMwareToolboxCmd.exe config get logging vmtoolsd.handler
```

Ejemplo de corrección mediante un comando de PowerCLI

```
VMwareToolboxCmd.exe config set logging vmsvc.handler syslog
VMwareToolboxCmd.exe config set logging toolboxcmd.handler syslog
```

```
VMwareToolboxCmd.exe config set logging vgauthsvc.handler syslog
VMwareToolboxCmd.exe config set logging vmtoolsd.handler syslog
```

Establecer la ubicación en vSphere Client

N/C

Asegurarse de que la versión de VMware Tools esté actualizada

El sistema operativo invitado debe asegurarse de que VMware Tools esté actualizado.

VMware Tools es una parte importante del ecosistema de VMware. Con VMware Tools puede administrar los sistemas operativos invitados, tales como:

- Apagado correcto
- Administración del ciclo de vida
- Obtener controladores para dispositivos paravirtualizados
- Personalizar e implementar plantillas de máquinas virtuales

Al igual que con todos los software, debe administrar y actualizar VMware Tools según sea necesario. Asegúrese de estar ejecutando una versión compatible del sistema operativo invitado, tanto si se proporciona como parte de la distribución de Linux como si lo instala para Microsoft Windows.

Valores

Valor predeterminado de instalación: N/D

Valor sugerido de línea base: N/D

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguno

Evaluación mediante comandos de PowerCLI

```
Get-VM -Name $VM | Select-Object -Property
Name,@{Name='ToolsVersion';Expression={$_.Guest.ToolsVersion}}
```

Ejemplo de corrección mediante un comando de PowerCLI

Específico del sitio. Existen varias formas de actualizar VMware Tools. Los controladores para VMXNET3 y PVSCSI también están disponibles a través de Windows Update, por lo que debe asegurarse de importarlos en herramientas como WSUS.

Establecer la ubicación en vSphere Client

Máquina virtual > Detalles de la máquina virtual > VMware Tools

Desactivar GlobalConf

El sistema operativo invitado debe desactivar GlobalConf, a menos que sea necesario.

La función GlobalConf de VMware Tools proporciona la capacidad de insertar configuraciones de archivos de `tools.conf` en las máquinas virtuales.

Valores

Valor predeterminado de instalación: False

Valor sugerido de línea base: False

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Los administradores deben utilizar otros métodos para actualizar y volver a configurar VMware Tools cuando sea necesario.

Evaluación mediante comandos de PowerCLI

```
VMwareToolboxCmd.exe config get globalconf enabled
```

Ejemplo de corrección mediante un comando de PowerCLI

```
VMwareToolboxCmd.exe config set globalconf enabled false
```

Establecer la ubicación en vSphere Client

N/C

Limitar la renovación automática de las funciones de VMware Tools

El sistema operativo invitado debe limitar la eliminación automática de funciones de VMware Tools.

Los procesos de actualización automática de VMware Tools pueden agregar o eliminar funciones de la instalación de VMware Tools, lo cual puede resultar útil, pero también presenta la oportunidad de alterar el perfil de seguridad del sistema operativo invitado desde vSphere.

Valores

Valor predeterminado de instalación: True

Valor sugerido de línea base: False

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Los administradores deben utilizar otros métodos para actualizar y volver a configurar VMware Tools cuando sea necesario.

Evaluación mediante comandos de PowerCLI

```
VMwareToolboxCmd.exe config get autoupgrade allow-remove-feature
```

Ejemplo de corrección mediante un comando de PowerCLI

```
VMwareToolboxCmd.exe config set autoupgrade allow-remove-feature false
```

Establecer la ubicación en vSphere Client

N/C

Configurar VMware Tools para actualizaciones automáticas

El sistema operativo invitado debe configurar las actualizaciones automáticas de VMware Tools según corresponda para el entorno.

vSphere puede iniciar las actualizaciones de VMware Tools, lo que puede resultar útil para mantener las versiones actuales de VMware Tools. Si administra y actualiza VMware Tools de otras maneras, desactive esta funcionalidad. En general, deje activadas las actualizaciones automáticas.

Valores

Valor predeterminado de instalación: True

Valor sugerido de línea base: true

Acción necesaria

Audite el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Los administradores deben utilizar otros métodos para actualizar y volver a configurar VMware Tools cuando sea necesario.

Evaluación mediante comandos de PowerCLI

```
VMwareToolboxCmd.exe config get autoupgrade allow-upgrade
```

Ejemplo de corrección mediante un comando de PowerCLI

```
VMwareToolboxCmd.exe config set autoupgrade allow-upgrade true
```

Establecer la ubicación en vSphere Client

N/C

Comprobar la versión de hardware de la máquina virtual

El sistema operativo invitado debe asegurarse de que la versión del hardware de la máquina virtual sea la 19 o posterior siempre que sea compatible.

El hardware 19 de la máquina virtual es compatible con ESXi 7.0 Update 2 y versiones posteriores. Las versiones más recientes del hardware de las máquinas virtuales habilitan nuevas funciones y un mejor rendimiento. Considere la posibilidad de actualizar a la versión 20 del hardware de la máquina virtual si está totalmente actualizado a vSphere 8.0 o una versión posterior. Como siempre, tenga cuidado al actualizar y pruebe por completo el proceso de actualización antes de implementarlo en todo el sistema.

Tenga en cuenta todas las ubicaciones en las que se puede ejecutar una máquina virtual o en las que es posible que necesite restaurar la máquina virtual. Por ejemplo, los usuarios del servicio VMware Cloud Disaster Recovery deben tener en cuenta los niveles de vSphere de SDDC de recuperación potenciales. Si bien VMware Cloud se ejecuta sobre vSphere, es posible que no tenga las mismas versiones de hardware virtual compatibles disponibles.

Los cambios en la configuración de los dispositivos virtuales suministrados por VMware no son compatibles y pueden provocar interrupciones en el servicio.

Nota Cuando se actualiza la versión de hardware de la máquina virtual, se producen actualizaciones de controladores y de otro tipo, aunque el impacto es mínimo.

Valores

Valor predeterminado de instalación: específico del sitio

Valor sugerido de línea base: vmx-19 o más reciente

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

El cambio de las versiones de hardware de la máquina virtual cambia las versiones de los dispositivos dentro del invitado, lo cual puede tener repercusiones. Pruebe siempre la actualización de las versiones de hardware virtual y recuerde que las instantáneas también capturan la versión de la máquina virtual para poder revertir las versiones si es necesario.

Los cambios en la configuración de los dispositivos virtuales suministrados por VMware no son compatibles y pueden provocar interrupciones en el servicio.

Evaluación mediante comandos de PowerCLI

```
(Get-VM -Name $VM | Get-View) | Select-Object -Property Name,@{Name='HW
Version';Expression={$_.Config.Version}}
```

Ejemplo de corrección mediante un comando de PowerCLI

```
Set-VM -VM $VM -HardwareVersion vmx-19
```

Establecer la ubicación en vSphere Client

Al crear una máquina virtual en el asistente Nueva máquina virtual, la opción **Seleccionar compatibilidad** establece la versión del hardware de la máquina virtual.

Referencia de controles de seguridad de vSAN

Estos controles de seguridad proporcionan un conjunto de líneas base de prácticas recomendadas para vSAN. Están estructurados de manera tal que se explican los beneficios y las compensaciones de la implementación del control. Para realizar cambios en estos controles, consulte la documentación de *Administrar VMware vSAN*.

Proteger datos en reposo

vSAN debe proteger los datos en reposo.

El cifrado de datos en reposo de vSAN ayuda a mantener la confidencialidad de los datos confidenciales mientras residen en dispositivos de almacenamiento y reduce el riesgo de acceso o exposición no autorizados en caso de pérdida o robo físico.

Puede cambiar este parámetro de configuración mientras el clúster está operativo. Al habilitar las protecciones de datos en reposo, se reformatean los grupos de discos (para vSAN OSA) y se vuelven a escribir los objetos almacenados (para vSAN ESA), lo que puede tardar mucho tiempo, pero se realiza en segundo plano. No es necesario apagar las cargas de trabajo. vSAN ESA 8.0 Update 2 introdujo la capacidad de habilitar protecciones de datos en reposo en un almacén de datos vSAN ESA existente. vSAN ESA 8.0 Update 3 introduce la capacidad de volver a deshabilitarla. Ejecute la versión más reciente de vSAN si utiliza ESA.

Valores

Valor predeterminado de instalación: desactivado

Valor sugerido de línea base: Habilitado

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Todo el cifrado se produce a costa de los ciclos de CPU y una posible latencia de almacenamiento. El impacto sobre las cargas de trabajo depende de diversos factores, como la configuración del hardware subyacente y el tipo y la frecuencia de E/S de almacenamiento por parte de la carga de trabajo.

Protección de datos al atravesar la red

vSAN debe proteger los datos en reposo, incluidas las comunicaciones de red relacionadas con el almacenamiento.

El cifrado de datos en tránsito de vSAN ayuda a garantizar que los datos confidenciales permanezcan confidenciales mientras atraviesan la red, lo que reduce el riesgo de interceptaciones o accesos no autorizados.

Puede modificar este parámetro de configuración mientras el clúster está operativo.

Valores

Valor predeterminado de instalación: desactivado

Valor sugerido de línea base: Habilitado

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Todo el cifrado se produce a costa de los ciclos de CPU y una posible latencia de almacenamiento. El impacto sobre las cargas de trabajo depende de diversos factores, como la configuración del hardware subyacente y el tipo y la frecuencia de E/S de almacenamiento por parte de la carga de trabajo.

Restringir el acceso a recursos compartidos de archivos NFS

Los recursos compartidos de archivos NFS en servicios de archivos de vSAN deben configurarse para restringir el acceso.

Al configurar un recurso compartido de archivos NFS, seleccione la opción "Personalizar el acceso a la red" y configure un conjunto restrictivo de permisos.

Valores

Valor predeterminado de instalación: sin acceso

Valor sugerido de línea base: Personalizar el acceso a la red

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Pérdida de conectividad con los clientes.

Cifrar autenticación SMB

Los recursos compartidos de archivos SMB en los servicios de archivos de vSAN solo deben aceptar comunicaciones con autenticación SMB cifradas.

Al configurar un recurso compartido de archivos SMB, active la opción Cifrado de protocolo (Protocol Encryption).

Valores

Valor predeterminado de instalación: desactivado

Valor sugerido de línea base: activado

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Ninguna.

Habilitar autenticación bidireccional/CHAP mutua

El destino iSCSI de vSAN debe habilitar la autenticación bidireccional/CHAP mutua.

El CHAP mutuo proporciona una capa adicional de protección, ya que requiere que tanto el iniciador (cliente) como el destino (servidor) verifiquen sus identidades entre sí, lo que garantiza que las entidades no autorizadas no intercepten ni alteren los datos transmitidos entre los dos.

Valores

Valor predeterminado de instalación: desactivado

Valor sugerido de línea base: activado

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Puede ser más difícil configurar los clientes.

Reservar espacio para completar operaciones de mantenimiento interno

vSAN debe reservar espacio para completar las operaciones de mantenimiento interno.

El ajuste de capacidad de reserva de operaciones de vSAN ayuda a garantizar que vSAN siempre tenga suficiente espacio libre para mantener la disponibilidad y la confiabilidad del almacén de datos de vSAN y evitar posibles pérdidas de datos o interrupciones del servicio debidas a una capacidad insuficiente durante las operaciones, como cambios de directivas.

Puede cambiar este parámetro de configuración mientras el clúster está operativo.

Valores

Valor predeterminado de instalación: desactivado

Valor sugerido de línea base: activado

Acción necesaria

Modifique el valor predeterminado de la instalación.

Impacto funcional potencial si se cambia el valor predeterminado

Al activar esta opción, se reduce la capacidad utilizable del almacén de datos de vSAN.

Acerca del Instituto nacional de estándares y tecnología

El instituto nacional de estándares y tecnología (National Institute of Standards and Technology, NIST) es un organismo público no regulador que desarrolla tecnología, métricas, estándares y directrices. La conformidad con estándares y directrices de NIST actualmente se ha convertido en una prioridad para muchos sectores.

El NIST se fundó en 1901 y ahora forma parte del departamento de comercio de EE. UU. El NIST es uno de los laboratorios de ciencias físicas más antiguos del país. Hoy en día, las mediciones del NIST admiten desde las tecnologías más pequeñas hasta las más grandes y complejas de las creaciones humanas, ya sean dispositivos a nanoescala, rascacielos antisísmicos o redes de comunicación global.

La Ley Federal de Administración de la Seguridad de la Información (Federal Information Security Management Act, FISMA) es una ley federal de Estados Unidos promulgada en 2002 a partir de la cual es un requisito que las agencias federales desarrollen, documenten e implementen un programa de seguridad y protección de la información. El NIST desempeña un papel importante en la implementación de la ley FISMA, ya que produce estándares y directrices de seguridad de claves (por ejemplo, FIPS 199, FIPS 200 y la serie SP 800).

El gobierno y las organizaciones privadas utilizan la base de datos NIST 800-53 para proteger los sistemas de información. La ciberseguridad y los controles de privacidad son esenciales para proteger las operaciones organizativas (incluidas su misión, sus funciones, su imagen y su reputación), los activos de la organización y a usuarios individuales frente a una amplia variedad de amenazas. Algunas de estas amenazas incluyen ataques cibernéticos hostiles, catástrofes naturales, fallas estructurales y errores humanos. VMware ha inscrito a un partner de auditoría externo para evaluar los productos y las soluciones de VMware mediante el catálogo de controles NIST 800-53. Para obtener más información, visite la página web del NIST en https://www.nist.gov/cyberframework.

Acerca de STIG de DISA

La Agencia de Sistemas de Información de Defensa (Defense Information Systems Agency, DISA) desarrolla y publica las guías de implementación técnica de seguridad (Security Technical Implementation Guides, STIG). Las STIG de DISA proporcionan instrucciones técnicas para fortalecer los sistemas y reducir las amenazas.

DISA es la agencia de apoyo de combate del DoD de EE. UU., responsable de mantener la posición de seguridad de la red de información del DoD (DoD Information Network, DODIN). Una de las formas en que DISA lleva a cabo esta tarea es desarrollando, difundiendo y exigiendo la implementación de STIG. En resumen, las STIG son guías portátiles basadas en estándares para fortalecer los sistemas. Las STIG son obligatorias para los sistemas de TI del DoD de EE. UU. y, como tales, proporcionan una línea base segura y verificada que permite a las entidades ajenas al DoD medir su situación de seguridad.

Los proveedores, como VMware, envían sugerencias para el refuerzo de la seguridad a la DISA para su evaluación, basándose en los protocolos y los comentarios de la DISA. Una vez completado ese proceso, se publica la STIG oficial en el sitio web de la organización DISA en https://public.cyber.mil/stigs/. Como parte de la *Guía de configuración de seguridad de vSphere*, VMware proporciona líneas base de seguridad y orientación para mejorar el fortalecimiento de vSphere. Consulte https://core.vmware.com/security.

Acerca de los CIP de NERC

North American Electric Reliability Corporation (NERC) es una autoridad regulatoria internacional sin fines de lucro que tiene la tarea de garantizar la confiabilidad y seguridad del sistema de energía a granel de América del Norte, incluidos los Estados Unidos, Canadá y parte de Baja California en México.

NERC desarrolla, aplica y supervisa los estándares de confiabilidad, y educa, capacita y certifica al personal de la industria. Los estándares de protección de infraestructura crítica (Critical Infrastructure Protection, CIP), un componente clave de las regulaciones de NERC, están diseñados para proteger los activos cibernéticos esenciales del sistema eléctrico a granel. Estos estándares exigen controles específicos de administración de seguridad, administración de seguridad del sistema, protección de la información y evaluaciones de vulnerabilidad para las utilidades y otras entidades dentro del sistema de energía a granel.

Para obtener más información, visite la página web de CIP de NERC: https://core.vmware.com/nerc-cip.

Acerca del ciclo de vida de desarrollo de seguridad de VMware

El programa de ciclo de vida de desarrollo de seguridad (Security Development Lifecycle, SDL) de VMware identifica y reduce los riesgos para la seguridad durante la fase de desarrollo de los productos de software de VMware. VMware también opera el centro de respuestas de

seguridad de VMware (VMware Security Response Center, VSRC) para llevar a cabo el análisis y la corrección de problemas de seguridad de software en los productos de VMware.

SDL es la metodología de desarrollo de software que el grupo de ingeniería de seguridad, comunicación y respuestas de VMware (VMware Security Engineering, Communication, and Response, vSECR) y los grupos de desarrollo de productos de VMware usan para ayudar a identificar y mitigar los problemas de seguridad. Para obtener más información sobre el ciclo de vida de desarrollo de seguridad de VMware, consulte la página web en https://www.vmware.com/security/sdl.html.

El VSRC trabaja con los clientes y la comunidad de investigación de seguridad para lograr los objetivos de solución de problemas de seguridad y para proporcionar a los clientes información práctica de seguridad de manera oportuna. Para obtener más información sobre el centro de respuestas de seguridad de VMware, consulte la página web en https://www.vmware.com/security/vsrc.html.

Registro de auditoría en vSphere

El registro de auditoría de tráfico de red, alertas de conformidad, actividad del firewall, cambios del sistema operativo y actividades de aprovisionamiento se considera una práctica recomendada para mantener la seguridad de cualquier entorno de TI. Además, el registro es un requisito específico de muchas de las normas y los estándares.

Uno de los primeros pasos que se deben tomar para garantizar que se está al tanto de los cambios en la infraestructura es auditar el entorno. De forma predeterminada, vSphere incluye herramientas que permiten ver y realizar un seguimiento de los cambios. Por ejemplo, puede utilizar la pestaña Tareas y eventos en vSphere Client para cualquier objeto en la jerarquía de vSphere a fin de ver los cambios producidos. También puede usar PowerCLI para recuperar eventos y tareas. Además, VMware Aria Operations for Logs ofrece un registro de auditoría para admitir la recopilación y retención de eventos importantes del sistema. Por último, hay muchas herramientas de terceros disponibles que proporcionan auditoría de vCenter Server.

Los archivos de registro también ayudan a determinar quién o qué tiene acceso a un host, una máquina virtual, etc. Para obtener más información, consulte Ubicaciones de archivos de registro de ESXi.

Eventos de auditoría de Single Sign-On

Los eventos de auditoría de Single Sign-On (SSO) son registros de acciones del usuario o del sistema para obtener acceso a los servicios de SSO.

vCenter Server 6.7 Update 2 y versiones posteriores mejora la auditoría de VMware vCenter Single Sign-On al agregar eventos para las siguientes operaciones:

- Administración de usuarios
- Inicio de sesión
- Creación de grupos

- Origen de identidad
- Actualizaciones de directivas

Los orígenes de identidades compatibles son vsphere.local, autenticación integrada de Windows (Integrated Windows Authentication, IWA) y Active Directory en LDAP.

Cuando un usuario inicia sesión en vCenter Server a través de Single Sign-On, o realiza cambios que afectan a SSO, se escriben los siguientes eventos de auditoría en el archivo de registro de auditoría de SSO:

- **Intentos de inicio y cierre de sesión:** los eventos para todas las operaciones de inicio y cierre de sesión correctas y con errores.
- **Cambio de privilegio:** los eventos de cambio en el rol o los permisos de un usuario.
- **Cambio de cuenta:** los eventos de cambio en la información de la cuenta de usuario, por ejemplo, nombre de usuario, contraseña u otra información adicional de la cuenta.
- **Cambio de seguridad:** los eventos de cambio en una configuración, un parámetro o una directiva de seguridad.
- **Cuenta habilitada o deshabilitada:** los eventos para cuando se activa o se desactiva una cuenta.
- **Origen de identidad:** los eventos para agregar, eliminar o editar un origen de identidad.

En vSphere Client, los datos de eventos se muestran en la pestaña **Supervisar**. Consulte la documentación de *Supervisión y rendimiento de vSphere*.

Los datos de eventos de auditoría de SSO incluyen los siguientes detalles:

- Marca de tiempo de cuando se produjo el evento.
- Usuario que realizó la acción.
- Descripción del evento.
- Gravedad del evento.
- Dirección IP del cliente utilizado para conectarse a vCenter Server, si está disponible.

Descripción general del registro de eventos de auditoría de SSO

El proceso de vSphere Single-Sign On escribe los eventos de auditoría en el archivo `audit_events.log` en el directorio `/var/log/audit/sso-events/`.

Precaución Nunca edite manualmente el archivo `audit_events.log`, ya que esto puede provocar un error en el registro de auditoría.

Al trabajar con el archivo `audit_events.log`, tenga en cuenta lo siguiente:

- El archivo de registro se archiva al alcanzar 50 MB.
- Se conservan 10 archivos de almacenamiento como máximo. Si se alcanza el límite, el archivo más antiguo se depura al crear un nuevo archivo.

- Los archivos llevan el nombre `audit_events-`<índice>`.log.gz`, donde el índice es un número del 1 al 10. El primer archivo que se crea es el índice 1 y ese número aumenta con cada archivo subsiguiente.
- Los eventos más antiguos se encuentran en el índice 1 del archivo. El archivo con el índice más alto es el archivo más reciente.

Descripción general de los próximos pasos de seguridad y conformidad

Llevar a cabo una evaluación de seguridad es el primer paso para la comprensión de las vulnerabilidades en la infraestructura. Una evaluación de seguridad forma parte de una auditoría de seguridad, en la que se analizan sistemas y prácticas, incluida la conformidad de seguridad.

Por lo general, una evaluación de seguridad hace referencia a examinar la infraestructura física de una organización (firewalls, redes, hardware, etc.) para identificar vulnerabilidades y defectos. Una evaluación de seguridad no es lo mismo que una auditoría de seguridad. Una auditoría de seguridad no solo abarca una revisión de la infraestructura física, sino también otras áreas como las directivas y los procedimientos operativos estándar, incluida la conformidad de seguridad. Una vez obtenida la auditoría, es posible decidir los pasos para solucionar los problemas dentro del sistema.

Durante la preparación para realizar una auditoría de seguridad, se pueden realizar estas preguntas generales:

1. ¿Nuestra organización tiene la obligación de seguir una norma de cumplimiento? De ser así, ¿cuál?
2. ¿Cuál es nuestro intervalo de auditoría?
3. ¿Cuál es nuestro intervalo de autoevaluación interna?
4. ¿Tenemos acceso a los resultados de auditoría anteriores y los hemos visto?
5. ¿Utilizamos una empresa de auditoría externa para prepararnos para una auditoría? De ser así, ¿cuál es su nivel de comodidad con la virtualización?
6. ¿Ejecutamos análisis de vulnerabilidad en los sistemas y las aplicaciones? ¿Cuándo y con qué frecuencia?
7. ¿Cuáles son nuestras directivas de ciberseguridad internas?
8. ¿El registro de auditoría se configuró según sus necesidades? Consulte Registro de auditoría en vSphere.

Si no existen instrucciones específicas o directrices sobre dónde empezar, es posible iniciar la protección del entorno de vSphere mediante las siguientes acciones:

- Mantener el entorno actualizado con las revisiones de software y firmware más recientes
- Mantener un nivel apropiado de protección y administración de contraseñas para todas las cuentas

- Revisar las recomendaciones de seguridad aprobadas por los proveedores
- Consultar las guías de configuración de seguridad de VMware (consulte Referencia de controles de seguridad de vSphere)
- Utilizar las instrucciones disponibles y comprobadas de marcos de directivas como NIST, ISO, etc.
- Seguir las instrucciones de los marcos de conformidad normativa como PCI, DISA y FedRAMP

vCenter Server y FIPS

En vSphere 7.0 Update 2 y versiones posteriores, puede habilitar la criptografía validada por FIPS en vCenter Server Appliance.

FIPS 140-2 es un estándar del gobierno de EE. UU. y Canadá que especifica los requisitos de seguridad para módulos criptográficos. vSphere utiliza módulos criptográficos validados por FIPS para que coincidan con los especificados en el estándar FIPS 140-2. vSphere tiene como objetivo ser compatible con FIPS para facilitar las actividades de cumplimiento y seguridad en varios entornos regulados.

En vSphere 6.7 y versiones posteriores, ESXi y vCenter Server usan criptografía validada por FIPS para proteger las interfaces de gestión y la VMware Certificate Authority (VMCA).

vSphere 7.0 Update 2 y versiones posteriores incluyen la criptografía validada por FIPS adicional en vCenter Server Appliance.

Nota vSphere favorece la compatibilidad con FIPS, por lo que algunos componentes deben tener en cuenta algunas consideraciones. Consulte Consideraciones al utilizar FIPS.

Módulos FIPS utilizados en ESXi

Un módulo criptográfico es un conjunto de hardware, software o firmware que implementa funciones de seguridad. ESXi utiliza varios módulos criptográficos validados por FIPS 140-2.

La siguiente tabla muestra el conjunto de módulos criptográficos validados por FIPS 140-2 que utiliza ESXi.

Tabla 17-3. Módulos FIPS

Módulo criptográfico	Versión	Algoritmos (CAVP)	Número de certificado
Módulo criptográfico de VMkernel	2.0	AES-CBC, AES-CBC-CS3, AES-CTR, AES-ECB, AES-GCM, AES-XTS Testing Revision 2.0, Counter DRBG, HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-512, SHA-1, SHA2-256, SHA2-512 (A2792)	Certificado en curso
Módulo de objetos FIPS de OpenSSL	3.0	AES, CKG, CVL, DRBG, DSA, ECDSA, HMAC, KAS-RSA-SSC, KAS-SSC, KBKDF, KDA, KMAC, KTS, KTS-RSA, PBKDF, RSA, SHA-3, SHS, Triple-DES (A1938)	Certificado n.º 4282
Módulo de objetos FIPS de VMware OpenSSL	2.0.20-vmw	AES, CKG, /drbg, DSA, ECDSA, HMAC, KAS-SSC, RSA, SHS, Triple-DES (C470)	Certificado n.º 3857
Módulo criptográfico ESXboot de VMware	1.0	HMAC-SHA2-224, RSA SigVer (FIPS186-4), SHA2-224, SHA2-256, SHA2-384, SHA2-512	Certificado n.º 4442
Módulo criptográfico Boring de VMware	6.0	AES, CVL, DRBG, ECDSA, HMAC, KAS, KAS-SSC, KTS, RSA, SHS, Triple-DES (A4970)	Certificado n.º 4694

Activar y desactivar FIPS en vCenter Server Appliance

Puede activar o desactivar la criptografía validada por FIPS en vCenter Server Appliance mediante solicitudes HTTP. La criptografía validada por FIPS está desactivada de forma predeterminada.

Puede utilizar varias formas de ejecutar solicitudes HTTP. Esta tarea muestra cómo utilizar el Centro para desarrolladores en vSphere Client para activar y desactivar la criptografía validada por FIPS en vCenter Server Appliance. Consulte *VMware vCenter Server Guía de programación de administración de* para obtener más información sobre el uso de las API de para trabajar con el vCenter Server Appliance.

Procedimiento

1 Inicie sesión en el sistema vCenter Server mediante vSphere Client.

2 En el menú, seleccione **Centro para desarrolladores**.

3 Haga clic en **API Explorer**.

4 En el menú desplegable **Seleccionar API**, elija **dispositivo**.

5 Desplácese hacia abajo por las categorías y expanda **system/security/global_fips**.

6 Expanda **GET** haga clic en **Ejecutar** en **Pruébelo**.

Puede ver la configuración actual en **Respuesta**.

7 Cambie la configuración.

a Para activar FIPS, expanda **PUT**, introduzca lo siguiente en el `request_body` y haga clic en **Ejecutar**.

```
{
"enabled":true
}
```

b Para desactivar FIPS, expanda **PUT**, introduzca lo siguiente en el `request_body` y haga clic en **Ejecutar**.

```
{
"enabled":false
}
```

Resultados

vCenter Server Appliance se reinicia después de activar o desactivar la criptografía validada por FIPS.

Consideraciones al utilizar FIPS

Al activar FIPS en vCenter Server Appliance, algunos componentes presentan restricciones funcionales actualmente.

No deben tenerse en cuenta las diferencias después de activar FIPS en vCenter Server, pero hay algunas consideraciones que se deben tener en cuenta.

Tabla 17-4. Consideraciones de FIPS

Producto o componente	Consideración	Solución alternativa
vCenter Single Sign-On	Cuando se activa FIPS, vCenter Server solo admite módulos criptográficos para la autenticación federada. Como resultado, RSA SecureID y algunas tarjetas CAC ya no funcionan.	Utilice la autenticación federada. Consulte la documentación de *Autenticación de vSphere* para obtener más detalles.
Complementos de la interfaz de usuario del cliente de vSphere que no son de VMware ni de sus socios	Es posible que estos complementos no funcionen con FIPS habilitado.	Actualice los complementos para usar bibliotecas de cifrado compatibles. Consulte el tema titulado "Preparar complementos locales para el cumplimiento de FIPS" en la documentación de *vSphere Client SDK*.
Certificados	No se probaron los certificados con tamaños de clave superiores a 3072 bits.	Genere certificados con claves de 2048 o 3072 bits.